

THINOMENON™

ACCESS
SUITE PREMIUM 2.0



User Manual

Thinomenon Access Suite User Manual

©2009-2011 Thinomenon All rights reserved.

Thinomenon, Inc.
480 Good Ave
Des Plaines, IL 60016

This document is being furnished by Thinomenon for informational purposes and only to licensed users of the Thinomenon Access Suite software product.

Efforts are made to ensure accuracy of the information presented. The content is subject to change without prior notice.

Changes, if any, will be incorporated in future releases.

All brands and product names are the trademarks or registered trademarks of the respective holders.

Microsoft is a registered trademark and Windows, Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Small Business Server 2003, Windows CE, Internet Explorer are the registered trademarks of the Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

Mac and Mac OS are trademarks of Apple Inc.

Unix is a registered trademark of the Open Group.

Pentium is a registered trademark of Intel Corporation.

AMD is a trademark of Advanced Micro Devices, Inc.

No part of this document may be reproduced for commercial purposes unless prior permission is obtained from the copyright holder.

Contents

1 Introduction

- 1.1 How to Use this Guide*
- 1.2 Introducing Thinomenon Access Suite*
- 1.3 Thinomenon Access Suite features*

2 Deploying Thinomenon Access Suite 2.0

- 2.1 Before You Start*
 - 2.1.1 Installation Overview*
- 2.2 Installing Thinomenon Access Suite*
 - 2.2.1 System requirements*
 - 2.2.2 Deploying All In One Installation configuration*
 - 2.2.3 Deploying Desktop Broker configuration*
 - 2.2.4 Deploying Advanced setup*
- 2.3 Updating Thinomenon Access Suite*
- 2.4 Uninstalling Thinomenon Access Suite*
- 2.5 Licensing*
 - 2.5.1 License Server*
 - 2.5.2 License information*
 - 2.5.3 Unlocking trial installation*
- 2.6 Troubleshooting*
 - 2.6.1 Thinomenon Access Suite logging*
 - 2.6.2 What to do if Management Console doesn't see Terminal Server*
 - 2.6.3 Creation of self-signed certificate with help of Thinomenon Certificate Tool*
 - 2.6.4 Check Farm Health Report*

3 Managing Server Software

- 3.1 Managing Farm-wide settings*
 - 3.1.1 Managing Virtual IP Address Configuration tab*
 - 3.1.2 Managing Virtual IP Processes*
 - 3.1.3 Change a Port for Load Balancing Gateway*
 - 3.1.4 Managing Web Access*
 - 3.1.5 Change Host Name*

3.1.6 Specify License Server

3.2 Managing Published Items

3.2.1 Publishing Desktop

3.2.2 Publishing the Application

3.2.3 Publish Document

3.2.4 Delete Published Items

3.2.5 Managing Filtration for Published items

3.3 Managing Administrative Privileges

3.3.1 Adding Administrators

3.3.2 Deleting Administrators

3.3.3 Managing Administrators Access to EMC Nodes

3.4 Managing of Installation Manager

3.5 Managing Isolation Environment

3.5.1 Adding New Isolation Environment

3.6 Smart Load-Balancing

3.6.1 Add Load Evaluator

3.6.2 Customizing Load Evaluator

3.6.3 Delete Load Evaluator

3.7 Managing Policies

3.8 Managing Printers

3.8.1 Setting a Default Printer

3.8.2 Clearing a Default Printer

3.8.3 Removing a Printer

3.8.4 Enabling Client Printing after Setup

3.8.5 Adding Published Printers

3.9 Managing Resource Manager

3.10 Managing Terminal Servers

3.10.1 Add Terminal Server

3.10.2 Connect to Added Terminal Server

3.10.3 Performing Server Maintenance

3.10.4 Managing Sessions

3.10.5 Virtual IP management

3.10.6 Managing Local Resources

3.11 Managing Other Computers node

3.11.1 Adding Computers to Other Computers node

3.11.1.1 Add computer by Browsing Network/Active Directory

3.11.1.2 Add computer by Name/IP

3.11.1.3 Add computer by IP Address Range

3.12 Working with Datacenters

3.12.1 Add Datacenter to EMC

3.12.2 Delete Datacenter from EMC

3.12.3 Modify Connection Properties of added Datacenters

3.12.4 Add/Delete Templates in Master Template list

3.12.5 Refresh list of VMs in Datacenter

3.12.6 Export list of VMs

3.12.7 Add Datacenter from Desktop Group creation wizard

3.13 Creating and Updating Desktop Groups

3.13.1 Create Persistent Desktop Group with Reprovision Logoff action for VDI

3.13.2 Create Persistent Desktop Group with No Logoff action for VDI

3.13.3 Create Persistent Desktop Group for Other/Physical

3.13.4 Create Temporary Desktop Group with Reprovision Logoff action for VDI

3.13.5 Create Temporary Desktop Group with No Logoff action for VDI

3.13.6 Create Temporary Desktop Group for Other/Physical

3.13.7 Modifying Desktop Group Properties

3.13.8 Deleting Desktop Group

3.14 Managing Computers in Desktop Groups

3.14.1 Adding Computers to Desktop Groups

3.14.2 Deleting Computers from Desktop Groups

3.15 Installing VDI Guest Tools

3.15.1 Manual VDI Guest Tools installation

3.15.2 Guest Tools installation in process of virtual machine creation

3.15.3 Guest Tools Installation from Management Console

3.16 Managing Sysprep Customization

3.16.1 Adding New Sysprep Customization

3.16.2 Modifying Sysprep Customization

3.16.3 Deleting Sysprep Customization

3.17 Managing Universal Printer Server options

3.17.1 Enable Server fonts redirection to Client

3.17.2 Enable adding remote session ID to printer names

3.17.3 Enable adding user name to printer names

3.17.4 Enable trace logging

4 Working with Client Software

4.1 Using Web Client

4.1.1 Overview

4.1.2 Usage

4.2 Using Thinomenon Access Client

4.2.1 Installing Thinomenon Access Client

4.2.2 Managing Thinomenon Access Client wide-options

4.2.3 Enable/Disable Status Bar

4.2.4 Change Startup option

4.2.5 Change Appearance option

4.3 Managing Connections

4.3.1 Add a New Connection

4.3.2 Modifying Connection Properties

4.3.3 Delete Connection

4.4 Working with Published items

4.4.1 Starting remote connection to published items

4.4.2 Create Shortcut of published items

4.4.3 Logoff/Disconnect sessions

4.5 Managing Universal Printer Client options

4.5.1 Enable Show Print options on this computer

4.5.2 Only redirect default printer

4.5.3 Save Printed pages in the EMF format

4.5.4 Enable trace logging

4.6 Uninstalling Thinomenon Access Suite client

5 Glossary

6 Appendix A

7 Appendix B

8 Appendix C

9 Appendix D

1 Introduction

1.1 How to Use this Guide

This manual describes Thinomenon Access Suite 2.0 for Windows®. Access Suite allows delivering Windows® desktops and applications on-demand to local and remote users on a variety of devices including PCs handheld, mobile, and embedded devices, running Windows®, Mac® OS X, Linux® and Unix® systems.

This manual is intended for system administrators who want to take advantage of the resource efficiency, robustness and security of the Thinomenon Access Suite for central deploying and provisioning seamlessly blended business applications.

About Thinomenon

Thinomenon, Inc. offers cloud infrastructure, desktop virtualization software solutions and related support and services. Thinomenon Access Suite allows hosting applications in private and public clouds on- and off-site and accessing these applications from any device including: PC, Mac, thin clients, Internet tablets, and Smartphones.

What problems do we solve?

IT departments spend majority of resources on maintenance. Maintaining individual desktops has become difficult and expensive. Thinomenon helps IT departments to transform business desktops into an on-demand utility-like service accessible from a wide variety of end-point computing devices, according to policies set in place by IT administrators. Thinomenon customers can decrease IT overhead shifting budgets towards improving business processes. Together with a network of system integrators and managed services providers, we make business computing more secure and agile.

Contact Thinomenon

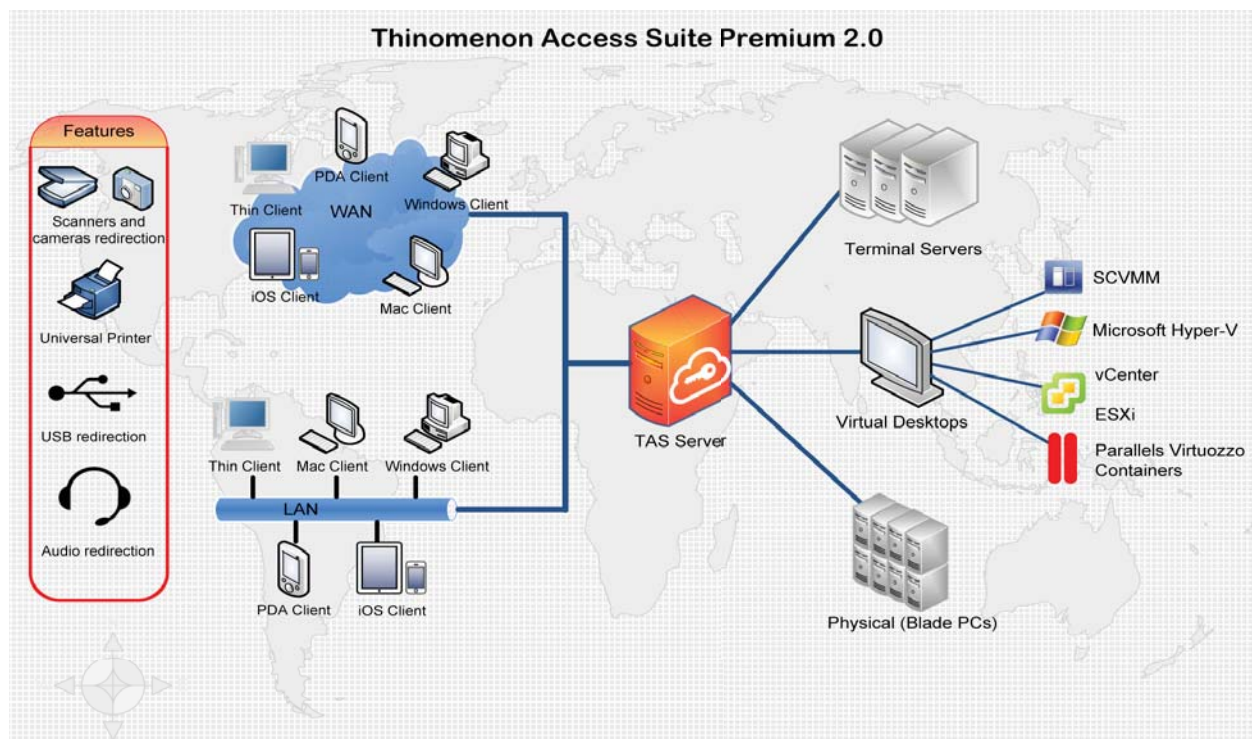
Web site	http://www.thinomenon.com/
Corporate Headquarters	Thinomenon, Inc. 480 Good Ave. Des Plaines, IL 60016 Tel: +1.847.859.3180
General information	info@thinomenon.com
Sales	sales@thinomenon.com

1.2 Introducing Thinomenon Access Suite

Thinomenon Access Suite 2.0 is a comprehensive Windows desktop and application delivery platform. It allows centralized deployment and provisioning of seamlessly blended applications, documents and user-desktops to any end-point device.

Thinomenon Access Suite is compatible with three Windows desktop models running on the back-end:

- Windows Terminal Services (Remote Desktop Services) also known as Server-Based Computing and Remote Desktop Session Host.
- Virtual Desktops hosted on hardware virtualization servers (VDI).
- Physical Computers such as Blade PCs.



Thinomenon Access Suite allows IT departments to provide end-users with secure access to business applications, regardless of users physical location. Thinomenon Access Suite separates office desktops from hardware, making it an ideal platform for telecommuting. Organizations where IT departments decide to go further can eliminate computer workstations altogether replacing them with virtual desktops accessed through inexpensive dumb terminals known as thin clients.

1.3 Thinomenon Access Suite features

Desktop and Application Publishing

Thinomenon Access Suite Premium allows publishing of full desktops, individual applications and documents from:

- Windows Terminal Services;
- Virtual Desktops hosted on hardware virtualization servers (VDI);
- Physical Computers (Blade PCs).

Resources hosted on terminal servers, hypervisors and blades could belong to the one/same Thinomenon farm.

Single point-and-click management interface - Intuitive all-in-one management allows administration of desktop, application and document access from a single easy-to-understand and use GUI console.

TWAIN scanners redirection - TWAIN scanner redirection allows on-demand applications and desktops to interact with TWAIN scanners locally attached to end-point access devices.

Two-directional high-quality local audio - High-definition local audio playback and recording makes on-demand desktops and applications multimedia compatible.

Universal Printer driver - Plug-and-Play local printer support lets remote applications utilize local printers. It provides on-the-wire font embedding, compression and advanced printing options support without having to install printer-specific drivers.

USB device redirection - Allows remote desktops to interact with USB devices attached to access devices.

IP address virtualization - Allows binding Remote Desktop Services (Terminal Services) sessions to unique IPs. This is necessary for enhanced legacy software compatibility.

Smart load-balancing - Allows administrators create flexible yet simple load-balancing policies for load distribution.

Administration delegation - Allows granting fine-grained administrative rights for managing Thinomenon Access Suite desktop farm.

2 Deploying Thinomenon Access Suite 2.0

2.1 Before You Start

2.1.1 Installation Overview

Components Overview

Access Suite is a modular platform. A solution is comprised from multiple components:

Management Tools: This component is necessary for configuration and administration of the Thinomenon farm. It has to be installed on a single computer (physical or virtual). This computer will be used to manage your Thinomenon farm. The following services are installed with Management Tools: *Thinomenon Database Agent Service*, *Thinomenon Software Update Service*.

Certificate Tool: This application is designed for making self-signed certificates. It is installed as a part of Management Tools.

Application Gateway: The application-layer gateway is an optional component that performs deep packet traffic inspection allowing multiple network streams to be forwarded through a single TCP port. The default port for Application Gateway is HTTPS (TCP 443). The following services are installed on the computer hosting Application Gateway: *Thinomenon Application Gateway Service*, *Thinomenon Software Update Service*.

Member Server: This component is an agent necessary to Access Suite to support terminal servers. It has to be installed on each server used for multiuser access. The following Windows Services are installed as parts of Member Server: *Thinomenon Agent*, *Thinomenon Intelligent RDP*¹, *Thinomenon TWAIN Redirector*, *Thinomenon Software Update*, *Thinomenon Taskbar Observer*, *Thinomenon Universal Printer*, and *Thinomenon Virtual IP*.

Load Balancer and Connection Broker: This component is used for distributing connections between hosts according to pre-assigned rules (filtering by terminal servers, Desktop Groups, load balancing rules, etc.) balancing system load while delivering proper desktops and applications to users. This component has to be installed on a single computer². The default port for Load Balancer and Connection Broker is TCP 4000. The following Windows Services come together with the Load Balancer and Connection Broker component: *Thinomenon Session Gateway*, *Thinomenon Software Update*.

License Server: Shares a pool of licenses on the network to be used by Member Servers and virtual/physical desktops. Hosts running License Server will have following Windows Services: *Thinomenon Licensing Server*, *Thinomenon Software Update*.

Web Portal: This component publishes available resources to end-users. The fol-

1 Installed only on Windows Server 2003 and Windows XP.

2 Starting with Access Suite 2.0 multiple load balancers are supported

lowing Windows Services come together with Web Portal: *Thinomenon Publishing Guard*, *Thinomenon Publishing Service*, and *Thinomenon Software Update*.

Guest Tools: These tools are installed on each virtual and physical machine in a managed desktop group. Serve as Access Suite agent on managed computers. The set of following Windows Services is installed with Guest Tools: *Thinomenon Remote USB Server*, *Thinomenon Agent*, *Thinomenon Intelligent RDP*, *Thinomenon TWAIN Redirector*, *Thinomenon Software Update*, *Thinomenon Taskbar Observer*, and *Thinomenon Universal Printer*.

Access Client – This is an installable receiving application providing access to their published desktops, applications and documents. The following Windows Services are installed with Access Client: *Thinomenon Credentials*, *Thinomenon Remote USB Client*.

Services Overview

Each Windows Services installed as a part of Thinomenon Access Suite performs a different function:

Thinomenon Database Agent: It's a Windows Service installed with the Management Tools component. It connects Thinomenon Access Suite modules to an internal database.

Thinomenon Software Update: This service monitors Thinomenon website for available software updates.

Thinomenon Application Gateway: This Windows Service performs deep TCP/IP traffic inspection, analyzing traffic in real-time. This allows sending several network streams through a single port.

Thinomenon Intelligent RDP: This Windows Service extends the RDP protocol allowing application publishing from Windows Server 2003. The Intelligent RDP service uses TCP port 8000 by default.

Thinomenon Agent: It collects the statistics for load evaluators, controls work of the *Allow only one instance* feature¹, sets the Firewall exceptions, checks user-permissions, and starts Windows Terminal Services if necessary.

Thinomenon TWAIN Redirector: It performs TWAIN scanner redirection.

Thinomenon Taskbar Observer: This service displays information about remote session (errors, warnings, etc.).

Thinomenon Universal Printer: This Windows Service is responsible for Plug-n-Playing printing.

Thinomenon Virtual IP: This component with virtual IP driver module are responsible for virtualization IP addresses of remote sessions.

Thinomenon Session Gateway: This Window service implements Load Balancer and Connection Broker functionality. It distributes the RDP-traffic taking into account the infrastructure (Terminal Servers, VDI, Physical/Blade PCs), filtering rules etc. By default, it uses port TCP 4000.

Thinomenon Publishing Guard: This component is necessary for the Web Portal configuration and certificate installation. It controls the state of the Thinomenon Publishing Service.

Thinomenon Publishing Service: This Windows Service comes as a part of Web Portal component. It serves delivering the list of published items to end-users.

Thinomenon Virtual USB Server: This Windows Service comes as a part of the Guest Tools component. It communicates with the Remote USB driver. By default, it listens on TCP 5000.

¹ The *Allow only one instance* feature controls the number of instances of the same application to be launched by the same user. For more details, please see *Working with Server Software -> Enterprise Management Console -> Published items* part of the manual.

Thinomenon Licensing Server: This service allows connecting to License Server remotely from other computers.

Thinomenon Credentials: This service comes as a part of Access Client and allows using Windows session credentials to connect to Thinomenon Farm.

Thinomenon Virtual USB Client: This Windows Service is installed as a part of Access Client. It connects to the Thinomenon Virtual USB Server and communicates with the Virtual USB driver.

Planning Deployment

Access Suite supports multiple backend platforms including: Windows Terminal Services starting with RDP 5.1, hypervisors including Microsoft® Hyper-V, Microsoft® SCVMM, VMware ESXi, VMware vCenter, and Parallels Virtuozzo Containers as well as physical computers including blade PCs.

Administrators should decide whether their business requirements dictate running terminal services, thus achieving maximum density and the highest possible ROI, server-hosted virtual desktops (VDI) or implementing a hybrid-approach providing power-users with blades and/or dedicated virtual machines, while using pooled virtual machines or hosting multiple sessions on single OS for lowest total cost of ownership when dedicated resources are not required.

Multiuser access to a single Operating System instance is usually the most efficient configuration, sufficient for majority or all end-users. Typically, multiuser access to Windows OS is provided using Windows Remote Desktop Services (formerly known as Windows Terminal Services).

Larger organizations, usually host their Remote Desktops on a load-balanced always-available server farm. Thinomenon platform allows centralized administration of such cluster from a single point-and-click interface. Administrators can work with individual nodes (member servers) applying important updates and restarting individual nodes without affecting overall availability.

Small organizations often deploy the All In One configuration on a single Windows server, taking advantage of on-demand computing without big investment in hardware.

In some situations, access to a standardized shared-resources server-based desktop will not be enough to meet the requirements of power users. This can happen due to multiple reasons including: a need for special dedicated hardware, elevated security concerns, a need to execute software incompatible with terminal services etc.

Thinomenon accommodates these users by delivering on-demand desktops hosted on dedicated and/or pooled Virtual Machines and physical PCs¹.

¹ Keep in mind that VDI deployments are usually bound by storage I/O throughput. To learn more about VDI storage design, read Thinomenon Blogosphere articles at <http://www.thinomenon.com/Blog/> as well as your storage vendor's literature.

There are following requirements for Thinomenon Access Suite deployment:

- To install Enterprise Management Console - single point of management for Thinomenon infrastructure – you need a computer (physical or virtual) running Microsoft Windows Server 2003 and higher. Application Gateway and Web Portal components have to be installed along with Enterprise Management Console;
- For **Remote Desktop Services** infrastructure - one or more physical or virtual machines running Microsoft Windows Server 2003 and higher with Remote Desktop Services (Terminal Services) role to install Member Server component. You can install Member Server to the same machine, where Enterprise Management Console is hosted;
- For **Virtual Desktops** hosted on **Microsoft SCVMM**, Microsoft .NET Framework (2.0 or later) and Microsoft Power Shell 2.0 must be installed on the server, where Management Console is hosted;
- For **Virtual Desktops** infrastructure with **VMware ESXi/VMware vCenter**²datacenter - VMware Virtual Disk Development Kit (VDDK) must be installed on the server, where Management Console is hosted. The path to VDDK bin directory must be added to the PATH environment variable. It is recommended to install VDDK before Thinomenon Management Tools installation³;

All necessary Firewall exceptions are created during installation.

Please note that Thinomenon Access Suite extends existing Windows security policies. Therefore, users need to have local login rights. Default Windows policy grants local login to members of Administrators and Remote Desktop Users groups.

² For more details about properly configure see Appendix A

³ For more details see Appendix B

2.2 Installing Thinomenon Access Suite

2.2.1 System requirements

Servers:

- 2-gigahertz (GHz) x86 and/or x64 Pentium 4-compatible or faster processors
- 2 gigabyte (GB) of RAM or more recommended
- Approximately 100 MB of available hard-disk space
- Windows® Server 2003, Windows® Server 2008, Windows® Server 2008 R2

Virtual Desktops:

- Microsoft Windows® XP, Microsoft Windows® Vista and Microsoft Windows® 7

Virtualization Platforms:

- Microsoft Hyper-V
- Microsoft SCVMM
- Parallels Virtuozzo Containers
- VMware ESXi
- VMware vCenter

Clients:

- Microsoft Windows 32/64-bit starting with Windows 2000
- Apple Mac OS X
- Apple iOS starting with 3.1 and higher
- Unix/Linux

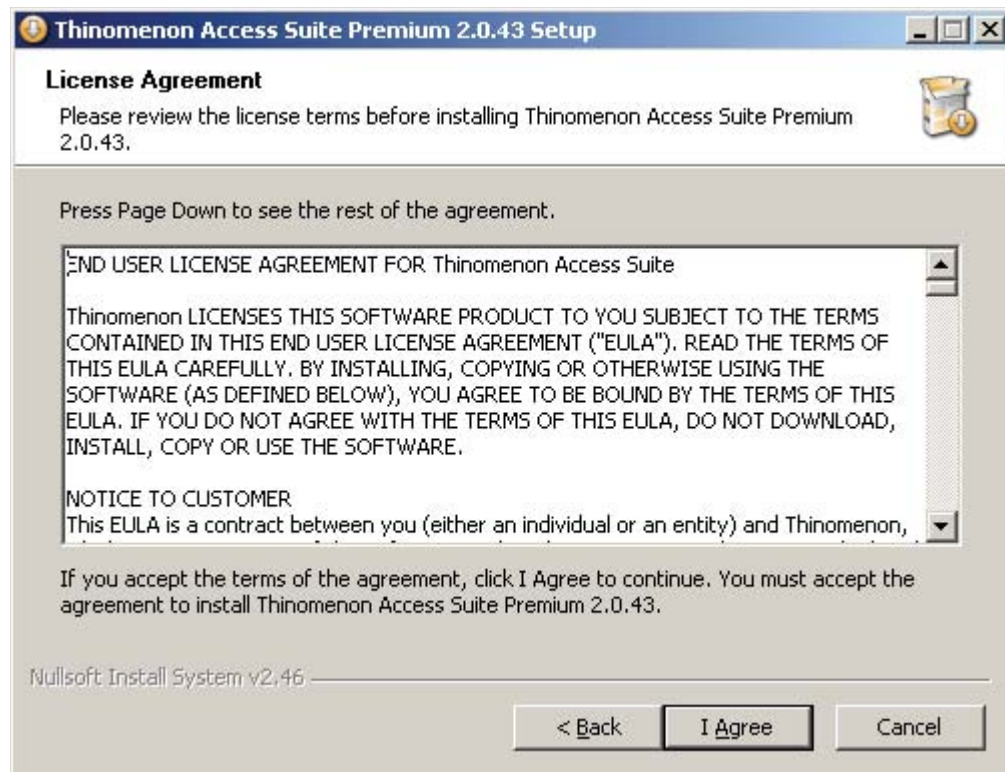
2.2.2 Deploying All In One configuration

To install the product with this type of installation:

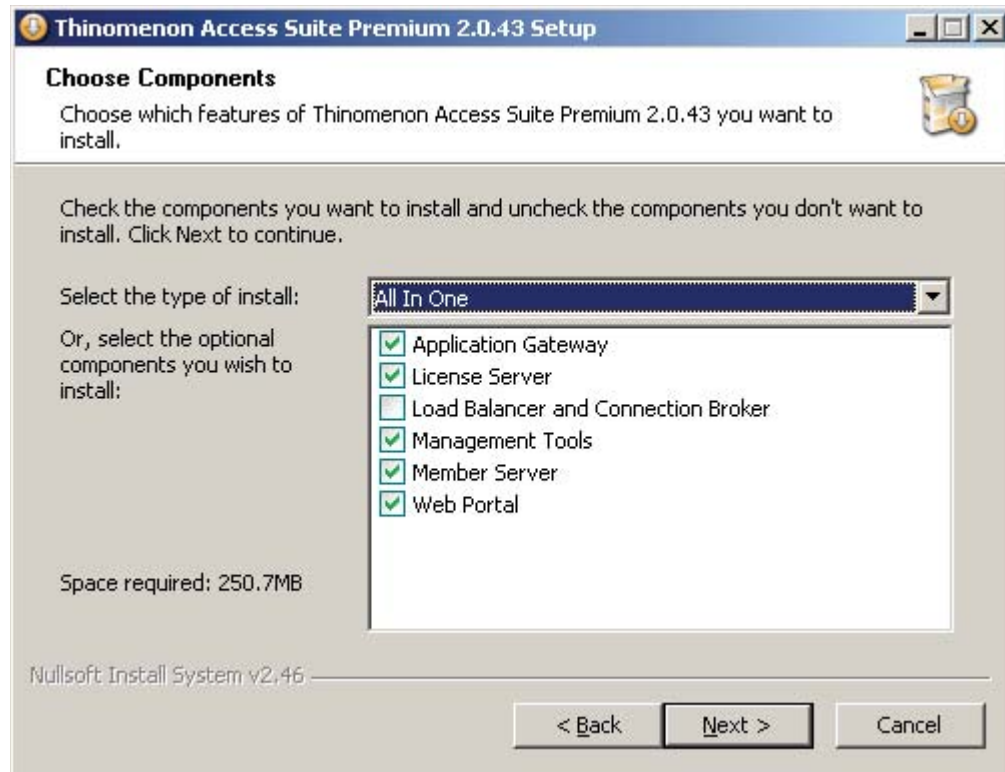
1. Start the application installer.
2. The *Thinomenon Access Suite Premium Setup* wizard opens. Click *Next*.



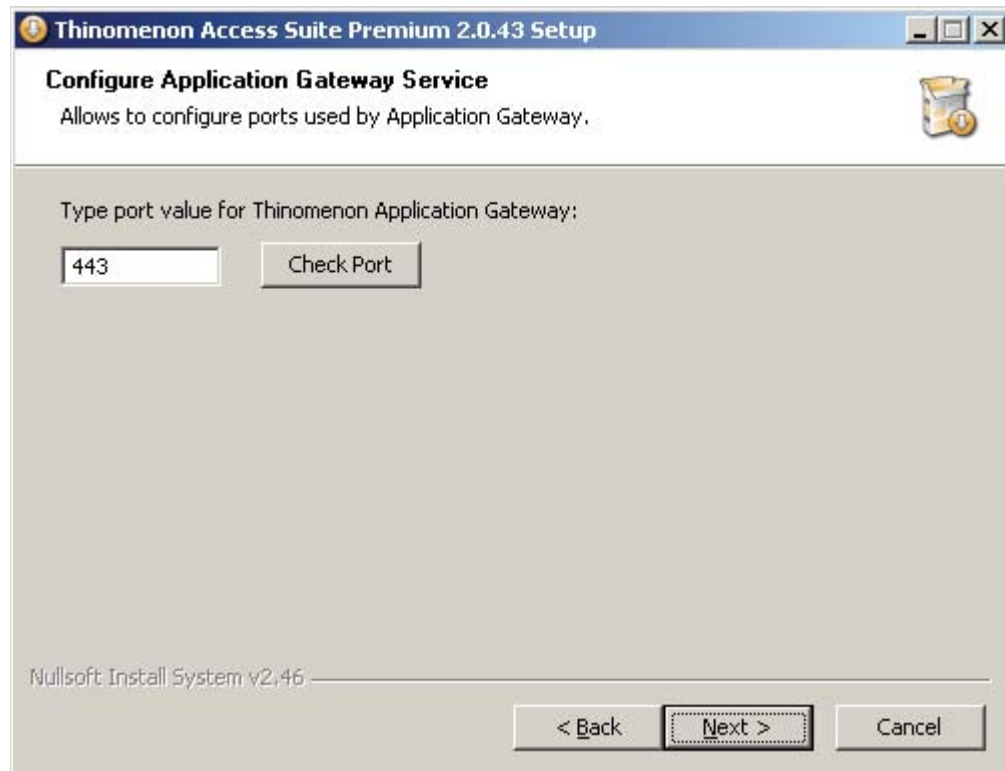
3. Read carefully the Thinomenon Access Suite End-user License Agreement and accept it. Click *Next*.



4. On the *Choose Components* page, select the *All In One* option from the drop-down configuration box. This will automatically select *Application Gateway*, *License Server*, *Management Tools*, *Member Server*, and *Web Portal* components while *Load Balancer and Connection Broker* will not be selected. Click *Next*.

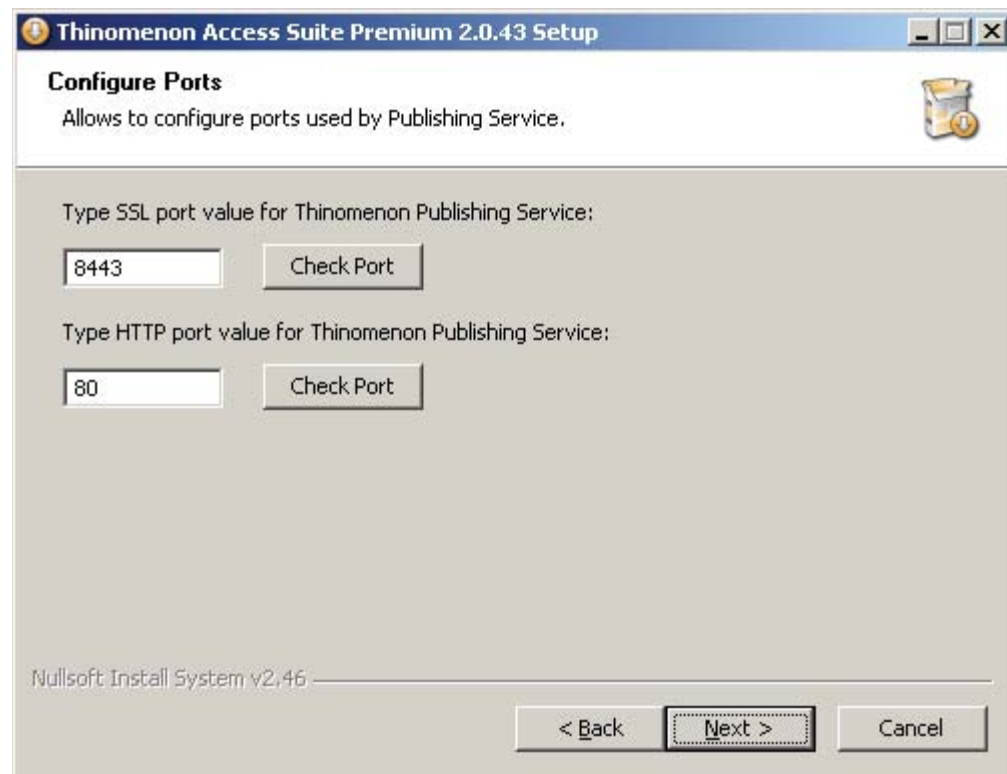


On the Configure Application Gateway Service page, select the port for the Application Gateway. Click **Check Port** to check if the port is open. Click **Next**.

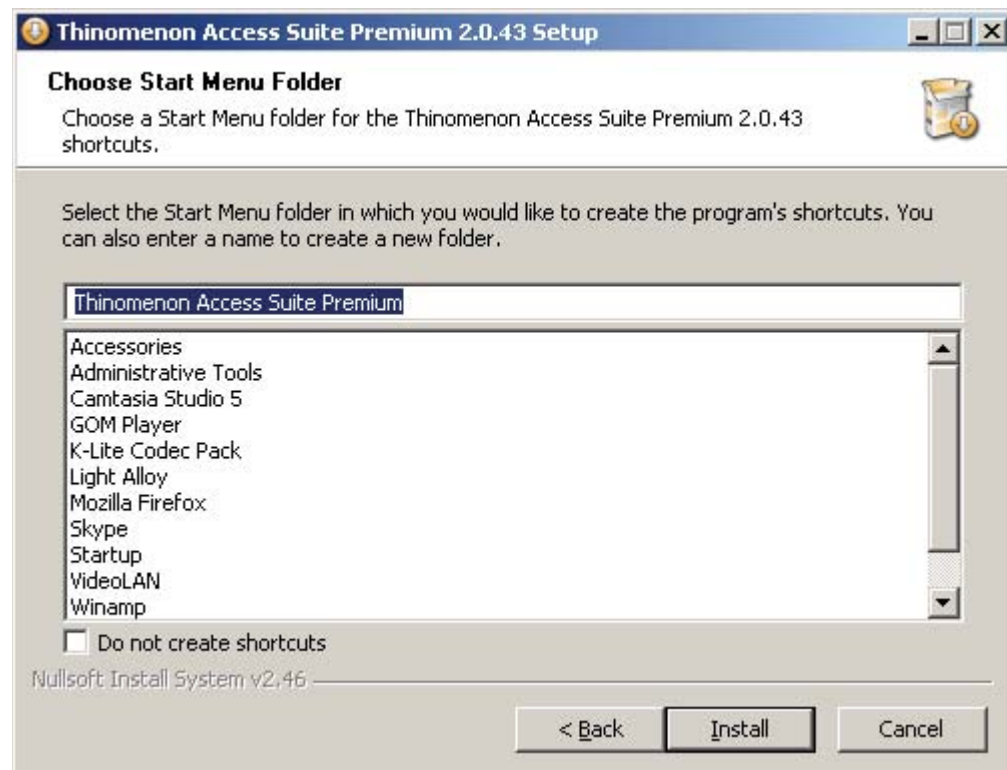


Choose SSL and HTTP ports for Thinomenon Publishing service. At least the HTTPS port has to be open for the software to interact with Thinomenon Access

Client⁴. Click **Check Port** to check if the port is open. Click **Next** to continue.

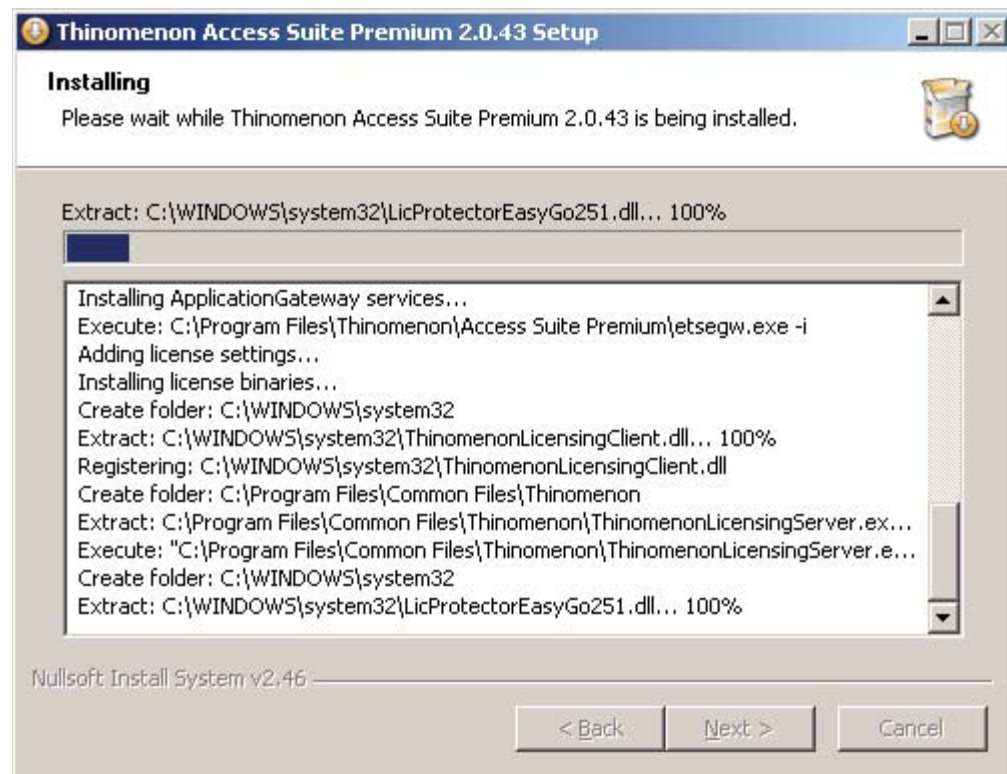


On the **Choose Start Menu Folder** page, define the name of Thinomenon Access Suite program group. Click **Next**.

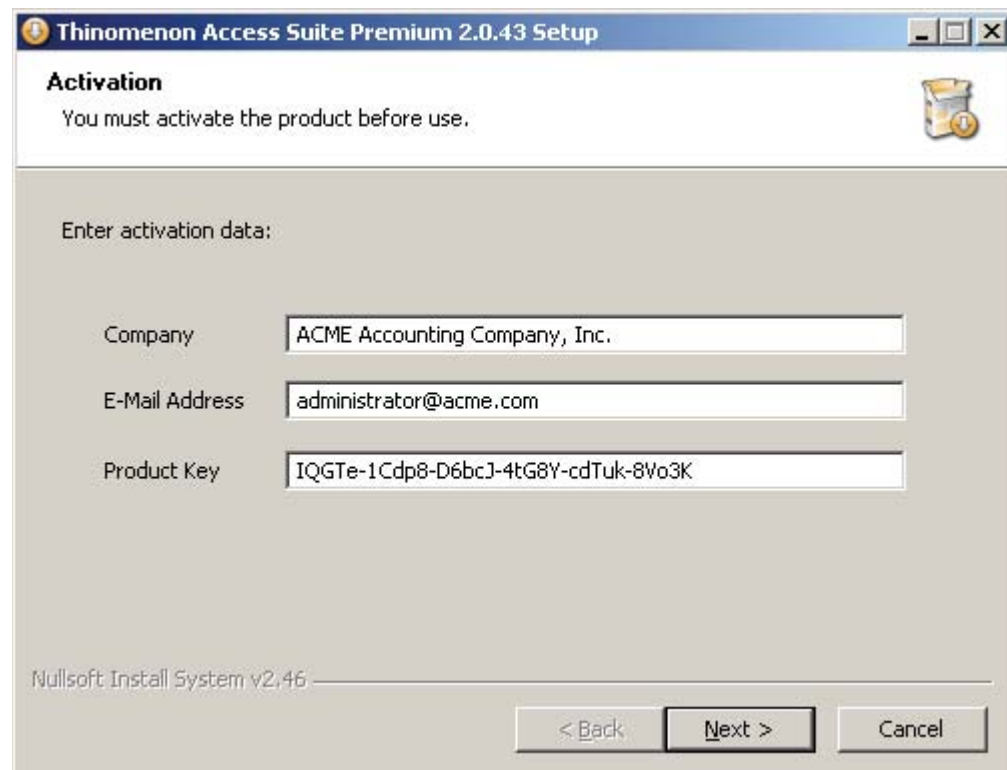


⁴ Thinomenon Intelligent RDP protocol is backwards compatible with Microsoft RDP. Legacy RDP client software will work.

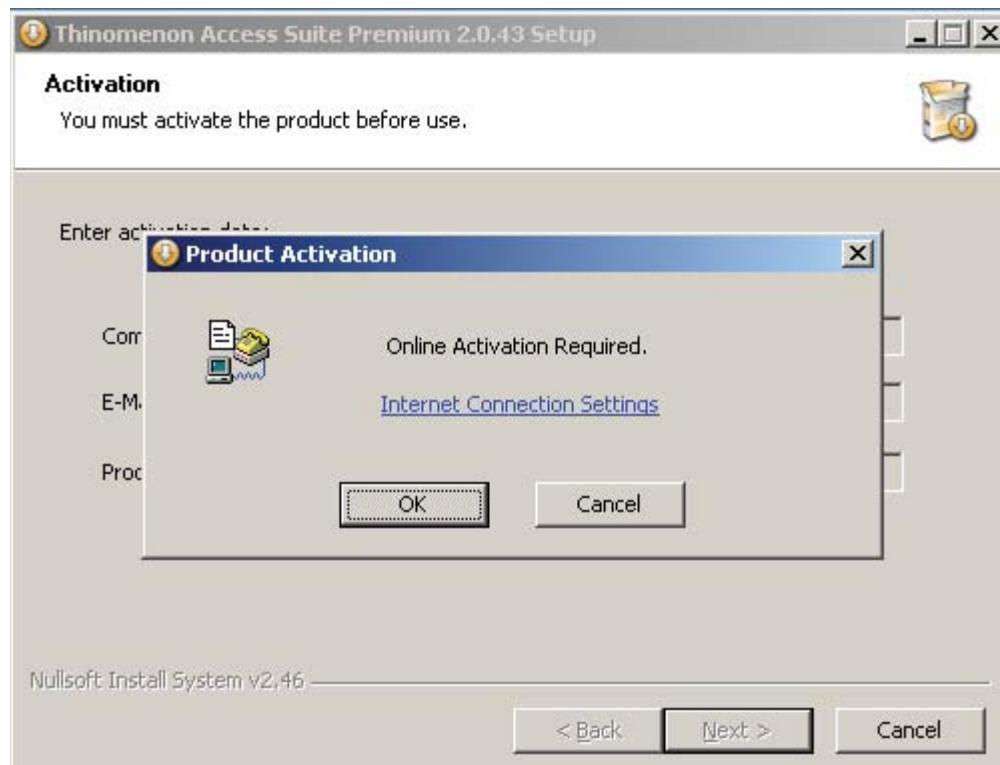
The installation starts.



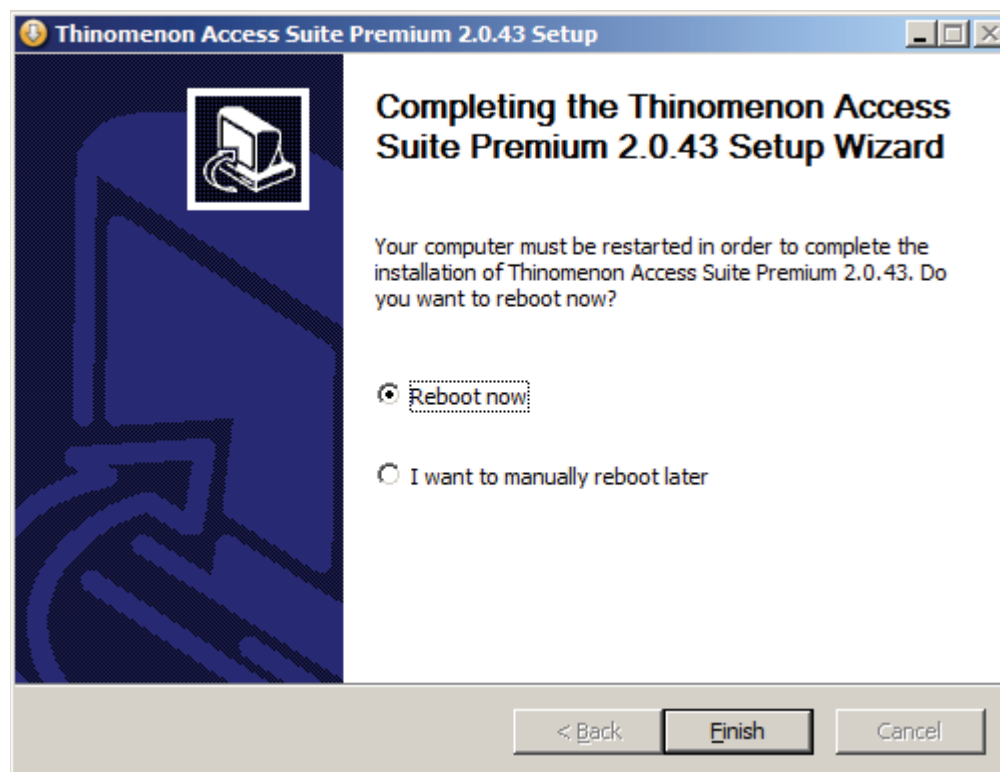
Once installation finishes, you will be prompted to enter the license information. Fill in the fields. Click *Next*.



Internet connection is required for the software to be activated. For alternative means to activate Access Suite, please contact Thinomenon sales.



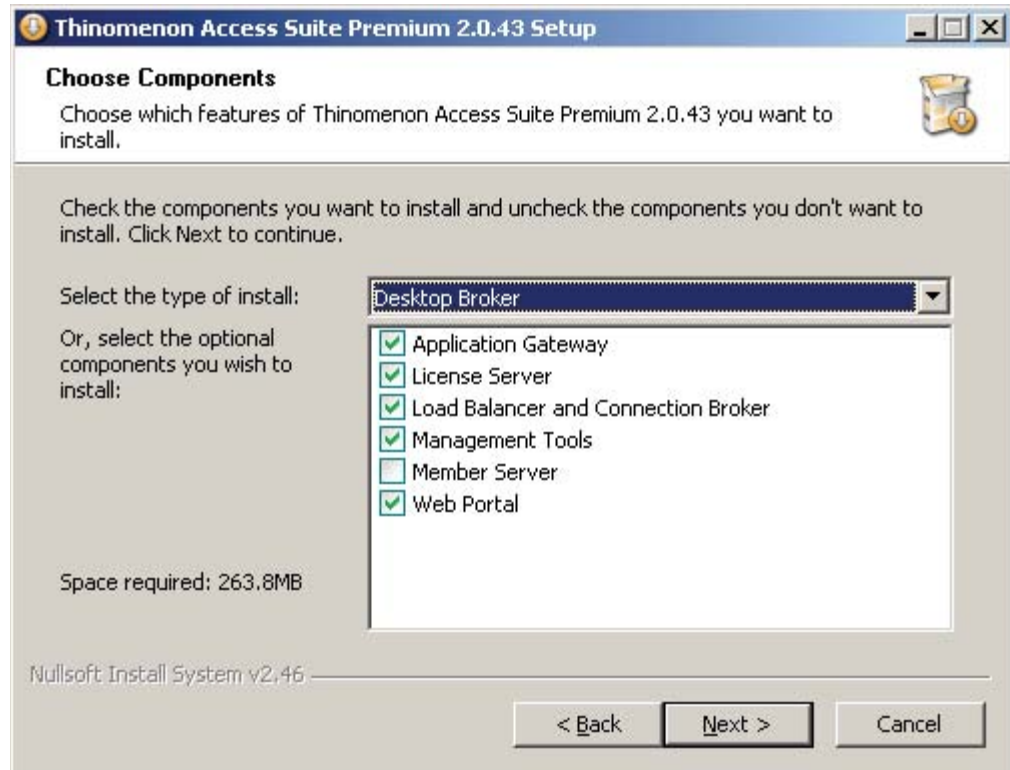
Once setup is complete, you might be asked to reboot your system. Select the reboot option and click **Finish**.



2.2.3 Deploying Desktop Broker configuration

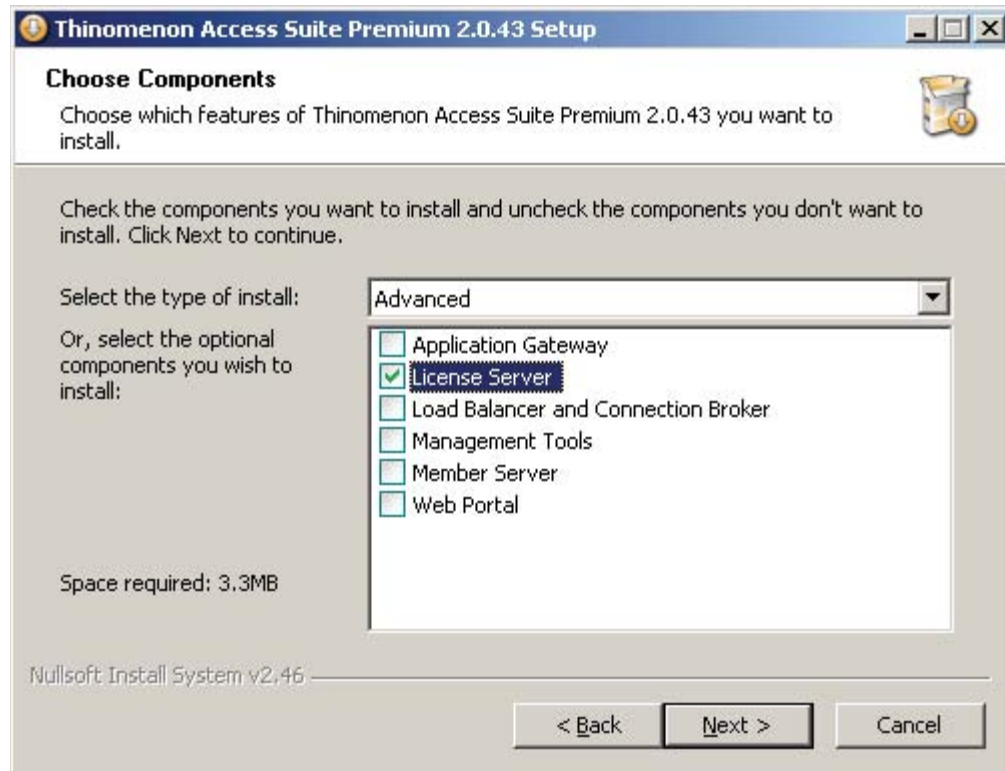
Desktop Broker is designed for managing Desktops infrastructure. It includes components to work with managed virtual desktops, physical computers and to manage member servers.

To install **Desktop Broker**, choose the appropriate option in the drop-down list. This will automatically preselect **Application Gateway**, **License Server**, **Load Balancer and Connection Broker**, **Management Tools**, and **Web Portal** components. Click **Next** and continue installation (see *All In One* installation type)



2.2.4 Deploying Advanced setup

The Advanced installation allows administrators to specify individual Access Suite components to be installed. For example, if it's necessary to install just the **License Server** component.

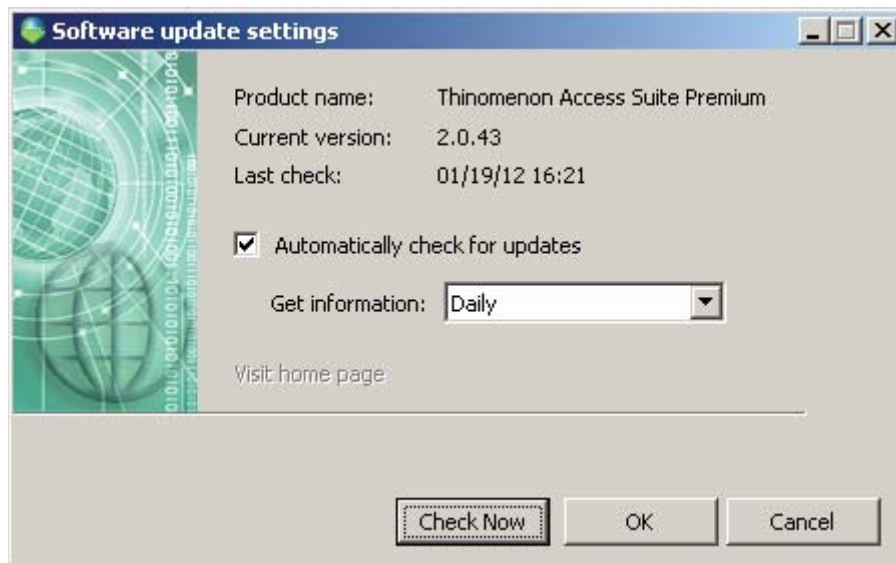


2.3 Updating Thinomenon Access Suite

Server-side components of Thinomenon Access Suite can be updated using the built-in software update module.

Thinomenon Software Update service monitors Thinomenon update server (by default office.thinomenon.com) for new update packages with the preset frequency.

To adjust update service settings launch *Automatic Update* from *Start menu* -> *Thinomenon Access Suite Premium*.

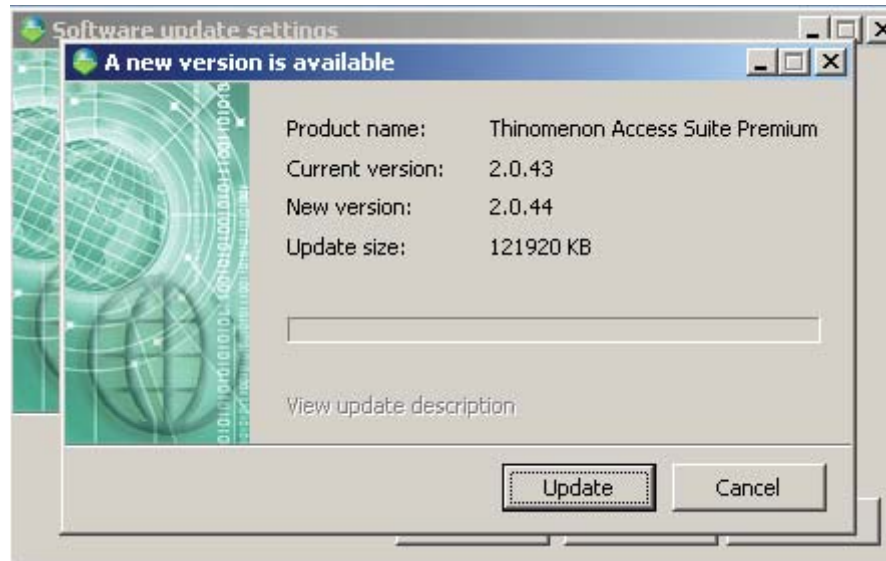


If the *Automatically check for updates* option is selected, notification about updates will be displayed automatically whenever an update is available.

To check for updates manually:

1. Select *Start menu* -> *Thinomenon Access Suite Premium*.
2. Click *Check Now*.

If an update is available, the following message will appear:

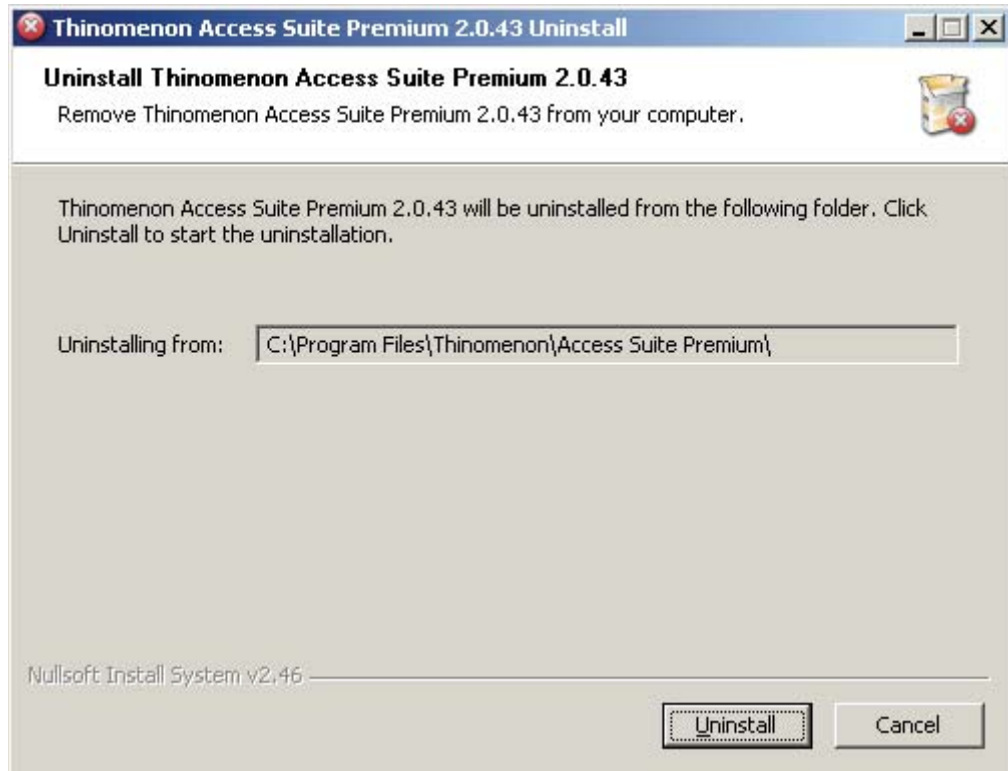


3. Click **Update** to start the update process.
4. Please reboot your computer after update is completed.

2.4 Uninstalling Thinomenon Access Suite

Thinomenon Access Suite could be removed from the system by invoking the uninstaller either from Add/Remove Programs application or by directly running uninstaller application from

Start -> Thinomenon Access Suite Premium -> Uninstall



Before the removal process begins, a user has to confirm that he/she wishes to uninstall the software.

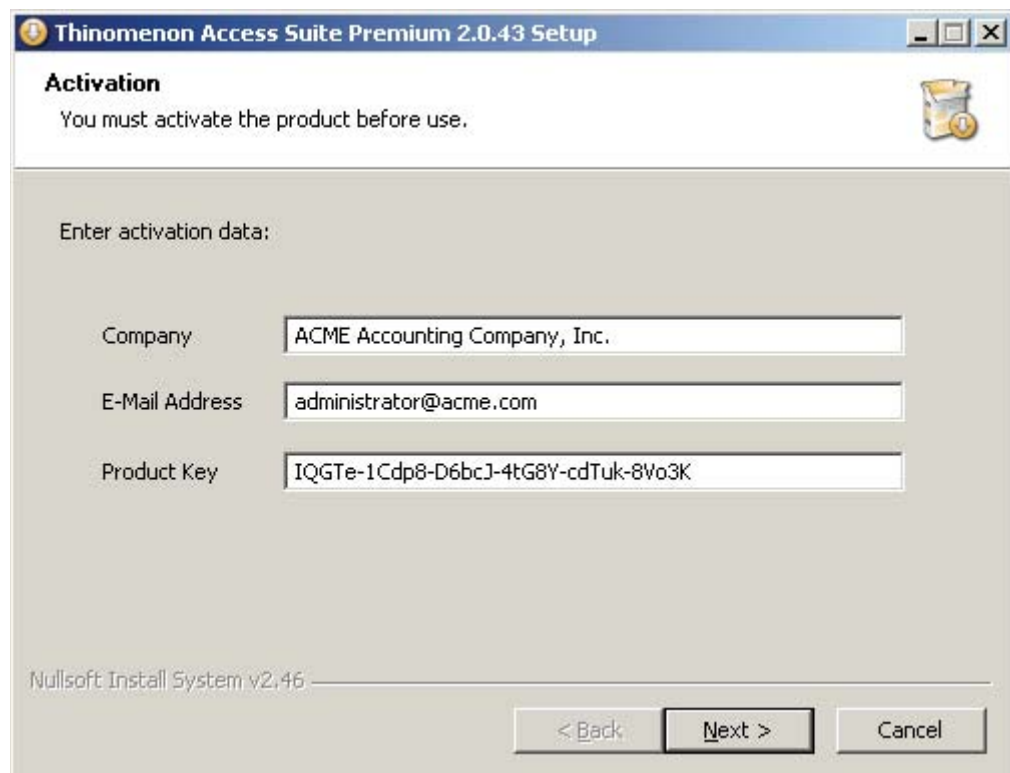
2.5 Licensing

Thinomenon Access Suite is licensed per concurrent connection. Any number of Terminal Servers, Virtual Desktops and Physical computers can belong to the Thinomenon farm according to this licensing model.

2.5.1 License Server

There is a licensing component called License Server. It shares a pool of connection licenses on the network. License Server is included into *All In One* and *Desktop Broker* configurations and it can be installed separately. You need one License Server per Thinomenon infrastructure.

After the License Server is installed, you have to activate it with the Product Key. The Internet connection is required for activation.

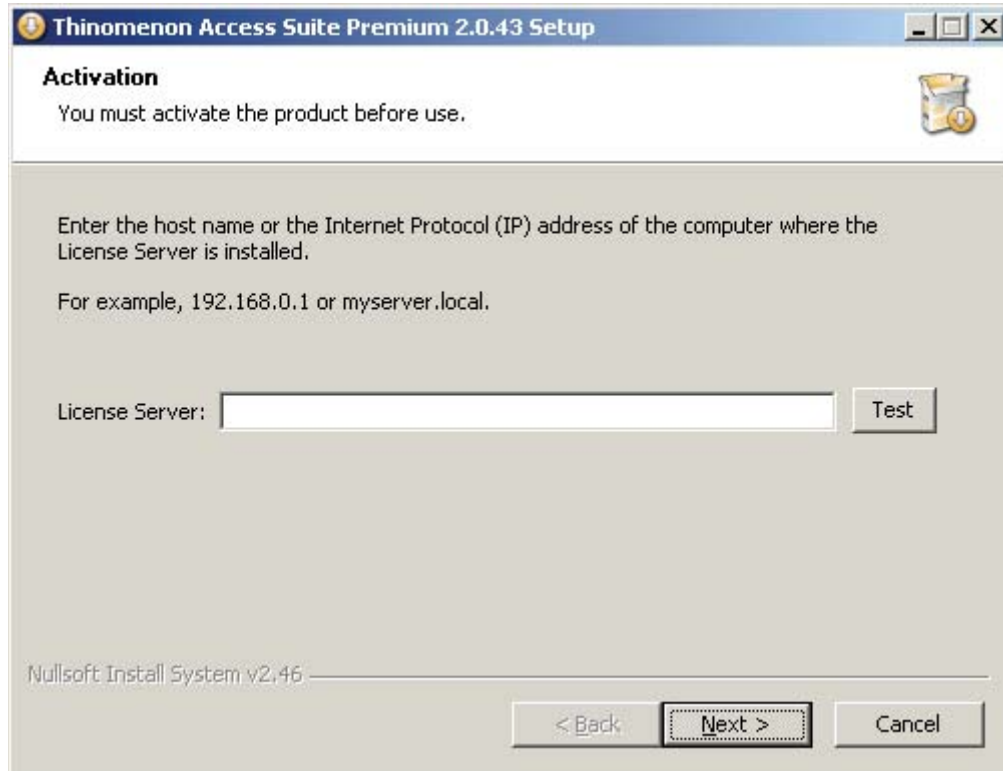


The screenshot shows the 'Activation' window of the 'Thinomenon Access Suite Premium 2.0.43 Setup' application. The window has a title bar with the application name and standard Windows window controls. Below the title bar, the word 'Activation' is displayed in bold, followed by the instruction 'You must activate the product before use.' and a small icon of a box with a question mark. The main area of the window is titled 'Enter activation data:' and contains three text input fields. The first field is labeled 'Company' and contains the text 'ACME Accounting Company, Inc.'. The second field is labeled 'E-Mail Address' and contains the text 'administrator@acme.com'. The third field is labeled 'Product Key' and contains the text 'IQGTe-1Cdp8-D6bcJ-4tG8Y-cdTuk-8Vo3K'. At the bottom of the window, there is a status bar that reads 'Nullsoft Install System v2.46'. To the right of the status bar are three buttons: '< Back', 'Next >', and 'Cancel'.

Once used, keys become tied to the host machine and cannot be applied to a different computer.

Once License Server was activated, it can be used to license clients embedded into Member Server and Guest Tools components.

During the Member Server component installation on a separate terminal server or manual Guest Tools installation, you'll be asked to enter the License Server information. Enter the IP address or the hostname of the machine, where License Server is installed.



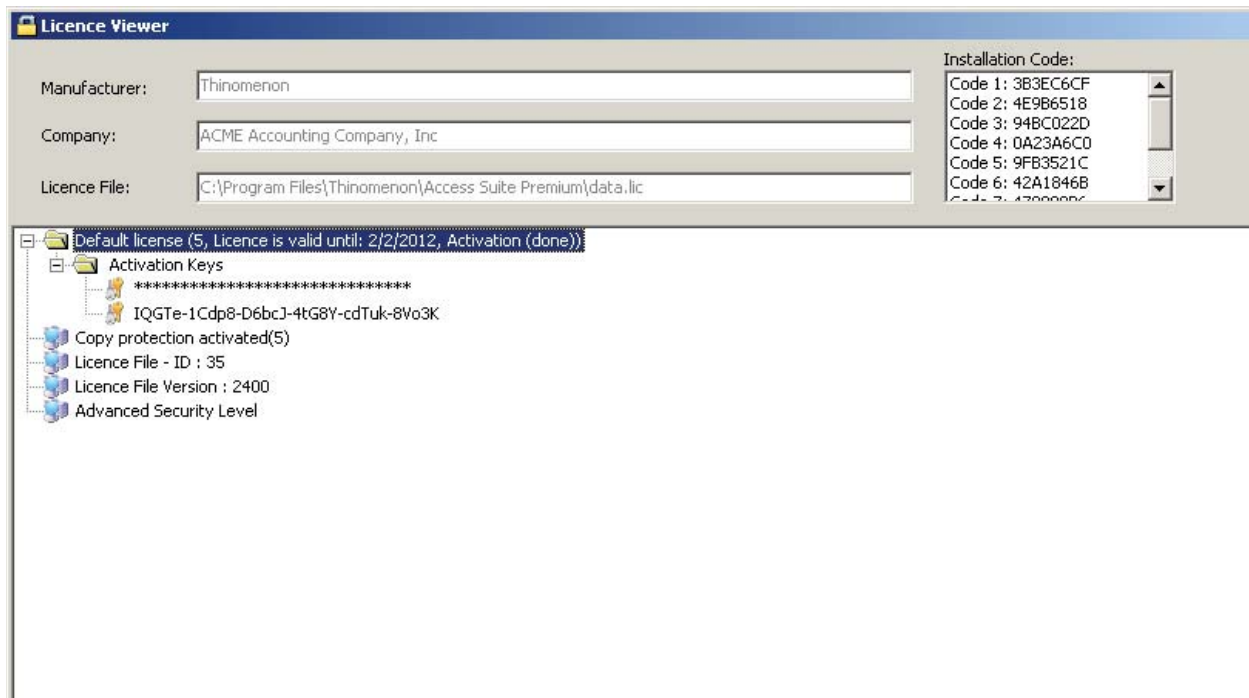
In case of automatic Guest Tools installation, the location of License Server will be detected automatically.

If License Server goes offline, all connected clients will continue working, but new connections won't be accepted.

2.5.2 License information

To see license information:

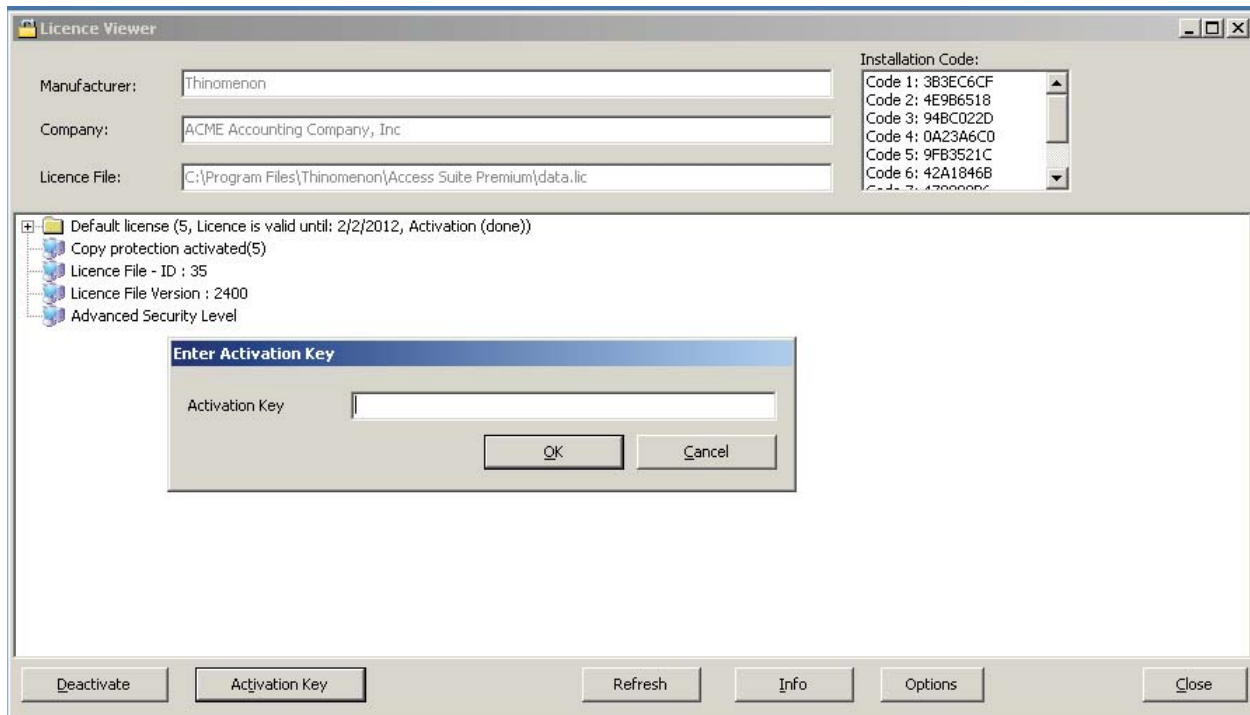
1. Select **Start menu -> All Programs-> Thinomenon Access Suite Premium -> Activation.**
2. The **License Viewer** window opens.
3. The license information is displayed in **Default license** node on the tree. It contains information about the number of licensed concurrent connections, and the expiration date if the product is licensed for evaluation.



2.5.3 Unlocking trial installation

To unlock a trial installation or add additional connection license keys:

1. Start **License Viewer** from **Start menu** -> **All Programs** -> **Thinomenon Access Suite Premium** -> **Activation**.
2. Click **Activation Key** in the bottom of the window.
3. Enter the activation key in the **Activation Key** field of the **Enter Activation Key** window and click **OK**.



2.6 Troubleshooting

2.6.1 Thinomenon Access Suite logging

Thinomenon Access Suite components can be configured to generate detailed debug logs. Ways to turn on logging for specific components are listed below:

Component	x86	X64	Additional
Application Gateway -RDPPProxy; -RDPShell;	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\RdpShell TraceLevel DWORD= 1 Log path: Documents and Settings\<USER>\Local Settings\Application Data\Thinomenon\Shell.log HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\RdpProxyService TraceLevel DWORD = 2 TraceRdp DWORD = 0x18 Log path: Default User\Local Settings\Application Data\Thinomenon	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Thinomenon\RdpShell TraceLevel DWORD= 1 Log path: C:\Documents and Settings\<USER>\Local Settings\Application Data\Thinomenon\Shell.log HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\RdpProxyService TraceLevel DWORD = 2 TraceRdp DWORD = 0x18 Log path: C:\Documents and Settings\Default User\Local Settings\Application Data\Thinomenon	<USER > - username which run the application.
Database agent	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS DBALogLevel DWORD = 1 Restart Thinomenon Database Agent Service Log path Default User\Application Data\Thinomenon\DBA 2008 Log path: C:\Windows\System32\config\systemprofile\AppData\Roaming\Thinomenon\DBA	HKEY_LOCAL_MACHINE\Software\Wow3264Node\Thinomenon\TAS DBALogLevel DWORD = 1 Restart Thinomenon Database Agent Service Log path: C:\Documents and Settings\Default User\Application Data\Thinomenon\DBA 2008 Log path: C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Thinomenon\DBA	
Access Client	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS Client LogLevel DWORD = 1 Restart Access Client Log path: Current user\AppData\Roaming\Thinomenon\TSEClient	HKEY_LOCAL_MACHINE\Software\Wow3264Node\Thinomenon\TAS Client LogLevel DWORD = 1 Restart Access Client Log path: Current user\AppData\Roaming\Thinomenon\TSEClient	

Load Balancer	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS LoadBalancerLogLevel DWORD = 1 And restart Thinomenon ETS Gateway service Log path: Default User\Application Data\Thinomenon\LoadBalancer 2008 Log path: C:\Windows\System32\config\systemprofile\AppData\Roaming\Thinomenon\LoadBalancer	HKEY_LOCAL_MACHINE \Software\Wow3264Node\Thinomenon\TAS LoadBalancerLogLevel DWORD = 1 And restart Thinomenon ETS Gateway service Log path: C:\Documents and Settings\Default User\Application Data\Thinomenon\LoadBalancer 2008 Log path: C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Thinomenon\LoadBalancer	
Universal Printer	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\Universal Printer TraceEnable = 1 Set the same key on client and server. Server system should be restarted. Log path <u>Server:</u> C:\Program Files\Thinomenon\Universal Printer\UPrinter.log <u>Client:</u> C:\Program Files\Thinomenon\Access Suite Client\Plugins\Universal Printer\UPrinter.log	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\Universal Printer TraceEnable = 1 Set the same key on client and server. Server system should be restarted. Log path <u>Server:</u> C:\Program Files (x86)\Thinomenon\Universal Printer <u>Client:</u> C:\Program Files (x86)\Thinomenon\Access Suite Client\Plugins\Universal Printer\UPrinter.log	
TWAIN Redirector	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\Remote Scanner LogLevel =5 Log path C:\Documents and Settings\<USER>\Application Data\Thinomenon\Remote Scanner 2008 Log path: C:\Windows\System32\config\systemprofile\AppData\Roaming\Thinomenon\Remote Scanner	HKEY_LOCAL_MACHINE \Software\Wow3264Node\Thinomenon\Remote Scanner LogLevel =5 Log path C:\Documents and Settings\<USER>\Application Data\Thinomenon\Remote Scanner 2008 Log path: C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Thinomenon\Remote Scanner	<USER> - username which run Remote Desktop and after that launch application which is using our redirected scanner
EMF-file	<u>On client:</u> HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\Universal Printer DumpMetaFileEnable = 1 EMF path: C:\Program Files\Thinomenon\Access Suite Client\Plugins\Universal Printer\DumpMetaFiles	<u>On client:</u> HKEY_LOCAL_MACHINE \Software\Wow3264Node\Thinomenon\Universal Printer DumpMetaFileEnable = 1 EMF path: C:\Program Files (x86)\Thinomenon\Access Suite Client\Plugins\Universal Printer\DumpMetaFiles	

Enterprise Management Console	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS EmconsoleLogLevel = 1 And restart EMConsole or server system. Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\EMConsole	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Thinomenon\TAS EmconsoleLogLevel = 1 And restart EMConsole or server system. 2008 Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\EMConsole	
Virtual Desktop	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS VirtualDesktopManagerLogLevel DWORD = 1 Log Path C:\Documents and Settings\%current user%\Application Data\Thinomenon\VirtualDesktopManager 2008 Log path: C:\Users\%current user%\AppData\Roaming\Thinomenon\VirtualDesktopManager	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Thinomenon\TAS VirtualDesktopManagerLogLevel DWORD = 1 Log Path C:\Documents and Settings\%current user%\Application Data\Thinomenon\VirtualDesktopManager 2008 Log path: C:\Users\%current user%\AppData\Roaming\Thinomenon\VirtualDesktopManager	
EsxProvider	HKEY_LOCAL_MACHINE \ SOFTWARE\Classes\CLSID\{47AB898F-D08D-4119-A896-35C0CDAF83B0}\Parameters If there no branch Parameters – create it Create string parameter LogFileName – with full path to log file. EnableLog DWORD=1	HKEY_LOCAL_MACHINE \ SOFTWARE\Wow3264Node\Classes\CLSID\{47AB898F-D08D-4119-A896-35C0CDAF83B0}\Parameters If there no branch Parameters – create it Create string parameter LogFileName – with full path to log file EnableLog DWORD=1	
HyperVProvider	HKEY_LOCAL_MACHINE \ SOFTWARE\Classes\CLSID \ {F5050EF5-D3EB-44F7-89B0-A898B597DEED}\Parameters If there no branch Parameters – create it Create string parameter LogFileName – with full path to log file EnableLog DWORD=1	HKEY_LOCAL_MACHINE \ SOFTWARE\Wow3264Node\Classes\CLSID \ {F5050EF5-D3EB-44F7-89B0-A898B597DEED}\Parameters If there no branch Parameters – create it Create string parameter LogFileName – with full path to log file EnableLog DWORD=1	
LoaderAddr	HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS LoaderAddrLogLevel = 1 Log path: C:\WINDOWS\system32\config\systemprofile\Application Data\Thinomenon\LoaderAddr 2008 Log path: C:\Windows\System32\config\systemprofile\AppData\Roaming\Thinomenon\LoaderAddr	HKEY_LOCAL_MACHINE \ Software\Wow3264Node\Thinomenon\TAS LoaderAddrLogLevel = 1 Log path: C:\WINDOWS\SysWOW64\config\systemprofile\Application Data\Thinomenon\LoaderAddr 2008 Log path: C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Thinomenon\LoaderAddr	

Virtual IP	1. Turn on Virtual IP Logging in properties of Terminal Server in EMC 2. Re-launch Thinomenon Virtual IP Service Log path: C:\Program Files\Thinomenon\Virtual IP\ elvipdrv.log	1. Turn on Virtual IP Logging in properties of Terminal Server in EMC 2. Re-launch Thinomenon Virtual IP Service Log path: C:\Program Files (x86)\Thinomenon\Virtual IP\ elvipdrv.log	
ERdpLauncher.exe	ERdpLauncher.exe places here: C:\WINDOWS\system32 Branch in registry: HKEY_LOCAL_MACHINE \ Software \ \Thinomenon\TAS ERdpLauncherLogLevel DWORD=1 Reboot System Log path: C:\Documents and Settings\<USER>\Application Data\Thinomenon 2008 Log path: C:\Users\<USER>\AppData\Roaming\Thinomenon\ERdpLauncher	ERdpLauncher.exe places here: C:\Windows\SysWOW64 Branch in registry: HKEY_LOCAL_MACHINE \ Software\Wow3264Node\Thinomenon\TAS ERdpLauncherLogLevel DWORD=1 Reboot System Log path: C:\Documents and Settings\<USER>\Application Data\Thinomenon\ERdpLauncher 2008 Log path: C:\Users\<USER>\AppData\Roaming\Thinomenon\ERdpLauncher	<USER > - username which run Remote Desktop.
Licensing	HKEY_LOCAL_MACHINE \ Software \ \Thinomenon\Licensing Server LicSrvLogLevel DWORD=1 Log path C:\Documents and Settings\%current user%\Application Data\Thinomenon\Licsrv 2008 Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\LicSrv	HKEY_LOCAL_MACHINE \ Software\Wow3264Node\Thinomenon\Licensing Server LicSrvLogLevel DWORD=1 Log path C:\Documents and Settings\%current user%\Application Data\Thinomenon\LicSrv 2008 Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\LicSrv	
Taskbar Tray	HKEY_LOCAL_MACHINE \ Software \ \Thinomenon\TAS TrayLogLevel DWORD=1 Log path C:\Documents and Settings\<USER>\Application Data\Thinomenon\TASTray 2008 Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\TASTray	HKEY_LOCAL_MACHINE \ Software\Wow3264Node\Thinomenon\TAS TrayLogLevel DWORD=1 Log path C:\Documents and Settings\<USER>\Application Data\Thinomenon\TASTray 2008 Log path C:\Users\%current user%\AppData\Roaming\Thinomenon\TASTray & C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Thinomenon\TASTray	<USER > - username which run Remote Desktop.

2.6.2 What to do if Management Console doesn't see Terminal Server

Hosts with Member Server component installed have an entry in Windows Registry, where name of a computer with Enterprise Management Console is stored:

HKEY_LOCAL_MACHINE\SOFTWARE\Thinomenon\TAS\ MemberServer-Owner

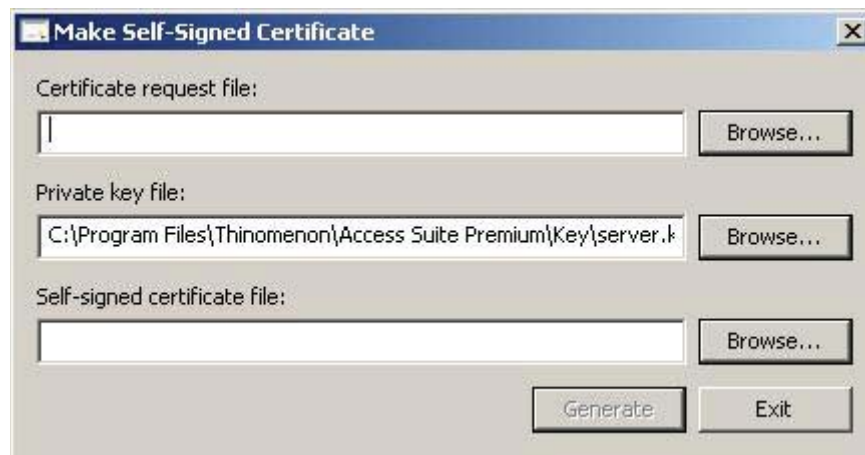
If you want to add Member Server to Enterprise Management Console, but you can't see you Member Server in the list of available servers, try going to Member Server's registry and deleting ***MemberServerOwner*** value. After that Member Server must appear in the list in Management Console.

2.6.3 Creation of self-signed certificate with help of Thinomenon Certificate Tool

If there no possibility to buy SSL certificate, you can create self-signed certificate using Certificate tool.

To create self-signed certificate:

1. Launch Certificate Tool from Start menu -> Thinomenon Access Suite Premium



2. Specify Certificate request file

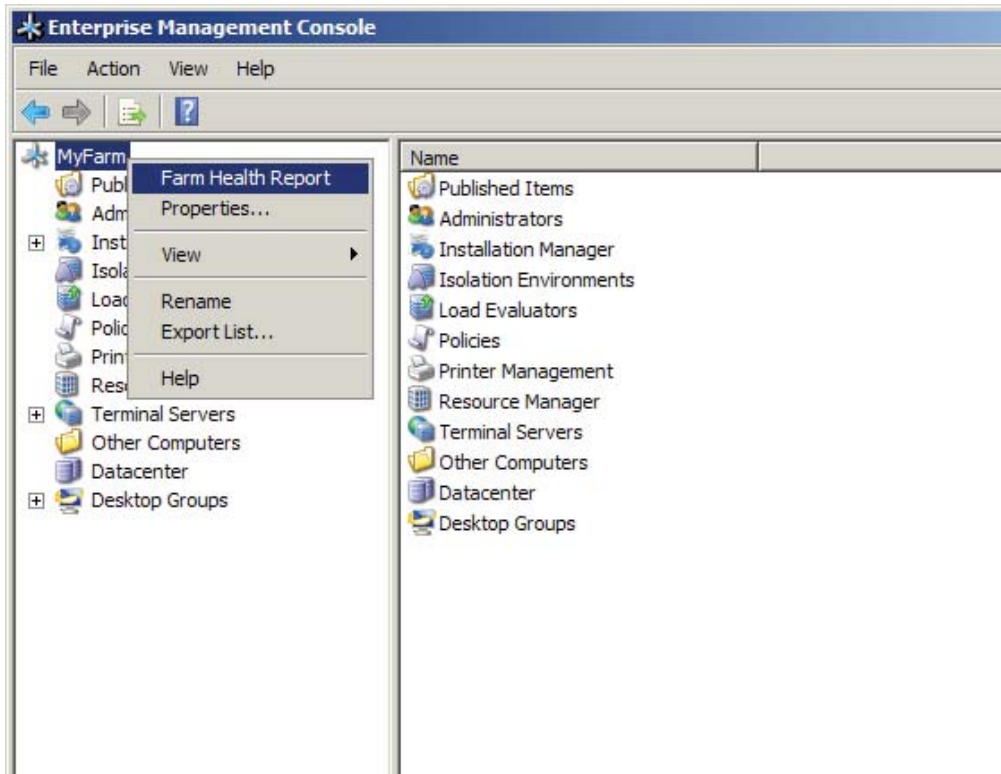
3. Specify path for Self-Signed Certificate file

4. Click Generate.

2.6.4 Check Farm Health Report

The Farm Health report displays information about the current state of Thinomenon Farm: installed Thinomenon components, state of Thinomenon services, etc.

To generate the Farm Health report, right-click the farm node and select the *Farm Health Report* item.



3 Managing Server Software

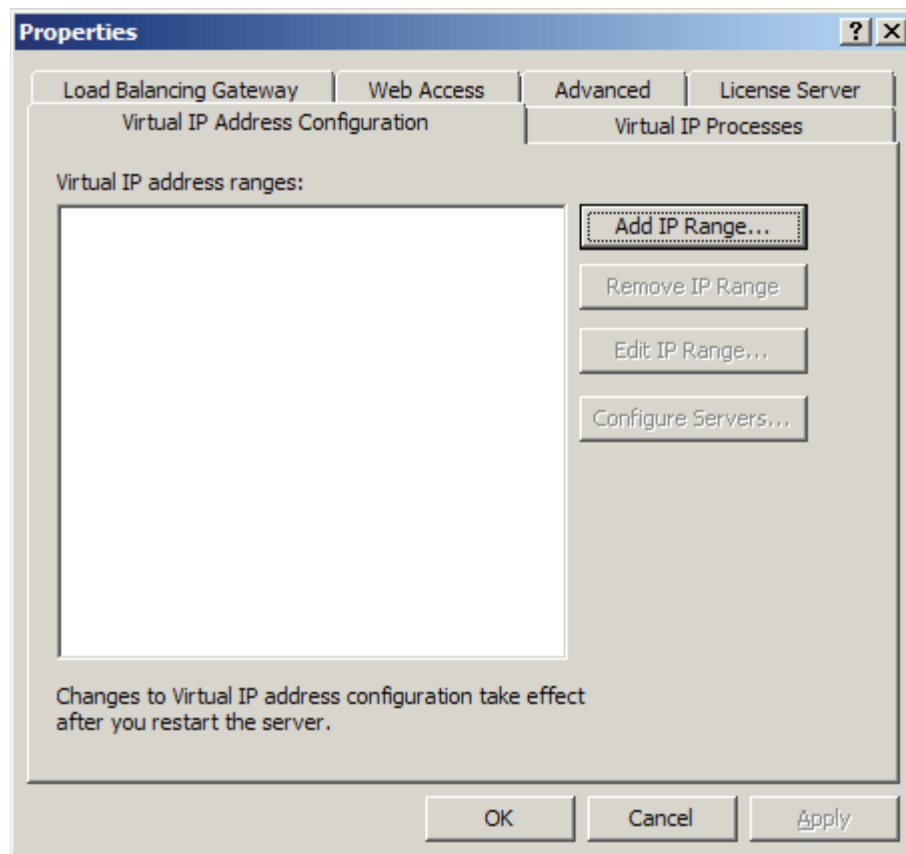
3.1 Managing Farm-wide settings

3.1.1 Managing Virtual IP Address Configuration tab

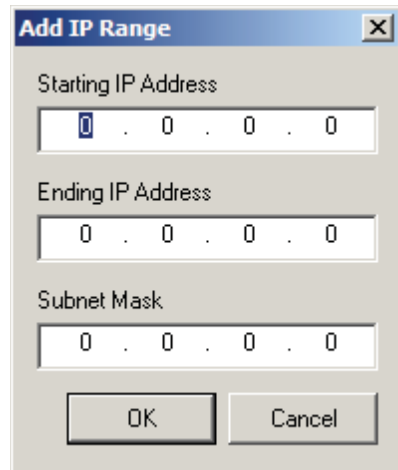
The **Virtual IP Address Configuration** tab concerns the Virtual IP configuration. On this tab you can define Terminal Servers to virtualize IP addresses for their remote sessions. Also you can assign a number of virtual IP addresses per server.

To configure IP addresses virtualization:

1. Open the **Virtual IP Address Configuration** tab and click **Add IP Range**.



2. Specify the range of IP addresses and click OK.

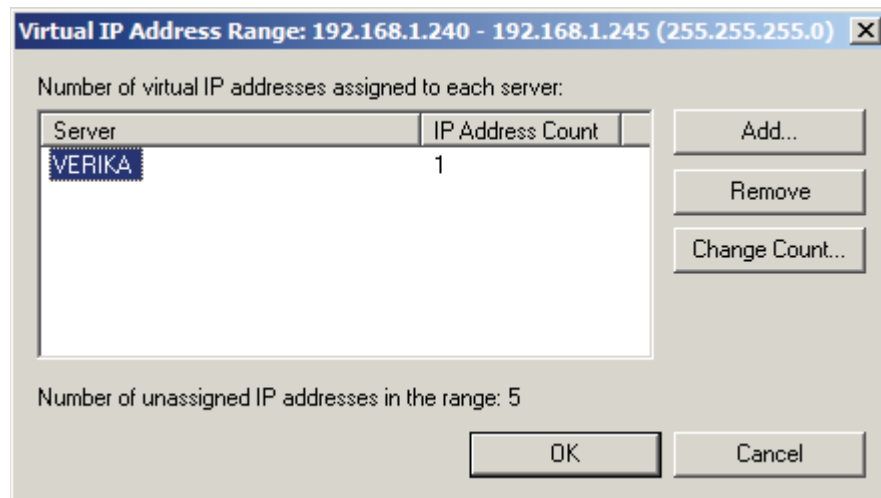


The 'Add IP Range' dialog box contains three input fields for IP addresses, each with a dotted separator. The 'Starting IP Address' field is pre-filled with '0'. The 'Ending IP Address' and 'Subnet Mask' fields are pre-filled with '0'. At the bottom are 'OK' and 'Cancel' buttons.

Field	Value
Starting IP Address	0 . 0 . 0 . 0
Ending IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0

3. You will be prompted to add Servers for this IP range. Click **Yes**, to start server adding. Please note you can add servers any time later by clicking **Configure servers**.

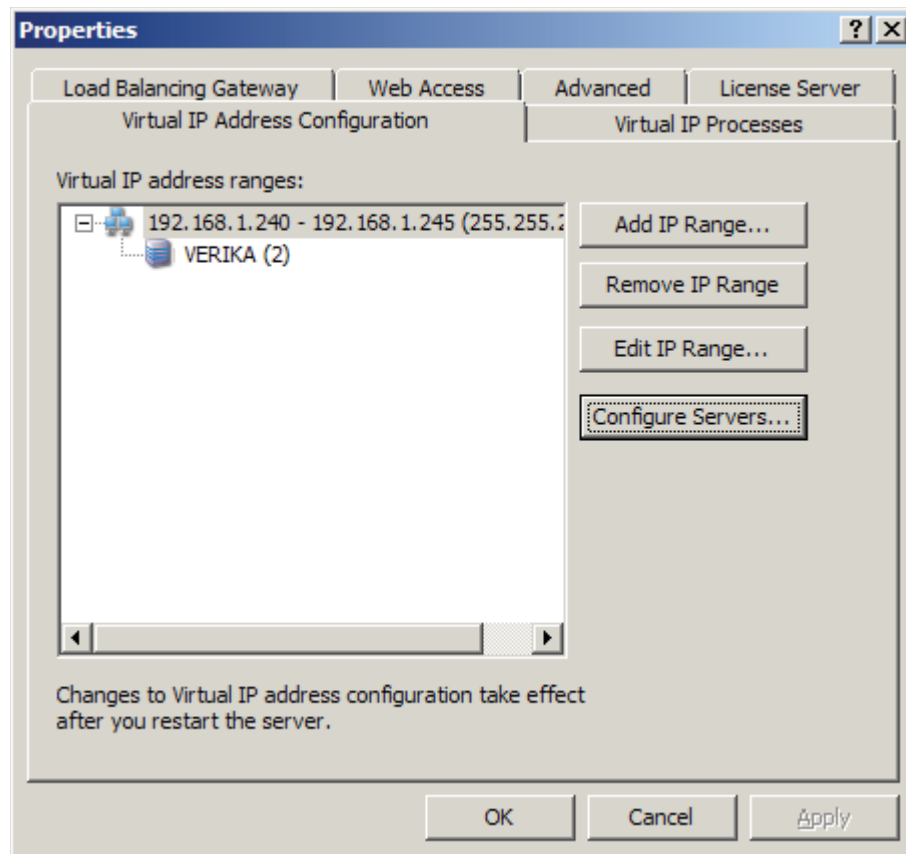
4. To configure servers, select the IP range and click **Configure Servers**. In the opened window, add servers by clicking **Add** and assign necessary number of IP addresses by clicking **Change Count**....



The 'Virtual IP Address Range' dialog box shows a table with one server named 'VERIKA' assigned 1 IP address. To the right are buttons for 'Add...', 'Remove', and 'Change Count...'. At the bottom, it shows 'Number of unassigned IP addresses in the range: 5' and 'OK'/'Cancel' buttons.

Server	IP Address Count
VERIKA	1

5. The server is added to the IP range.

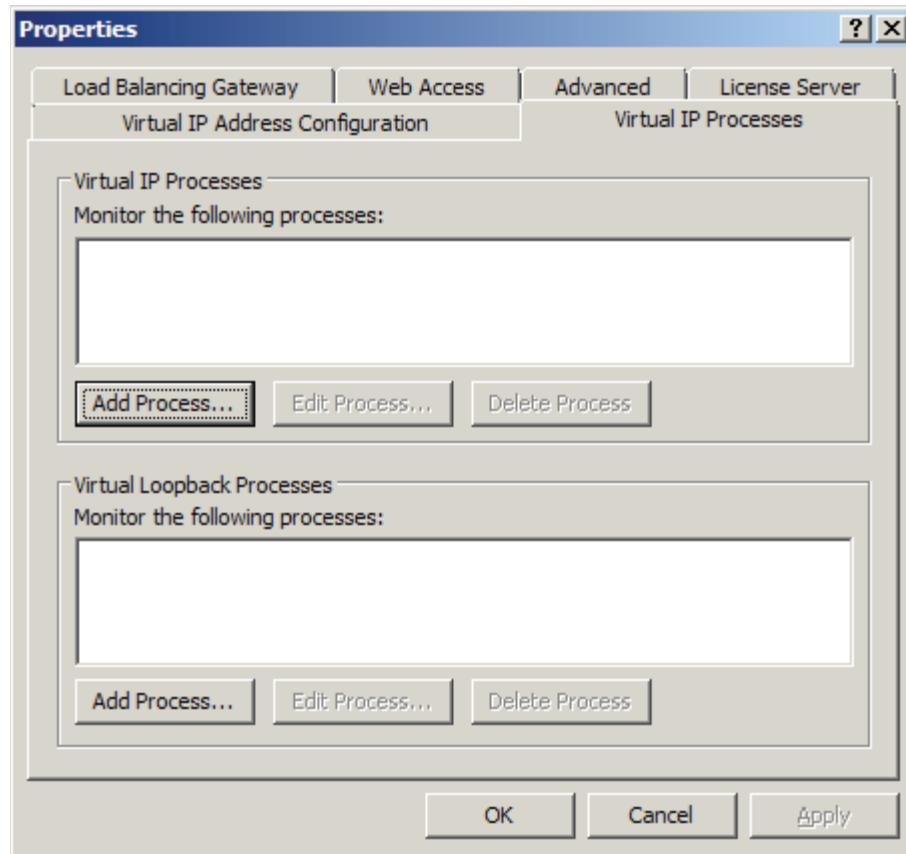


3.1.2 Managing Virtual IP Processes

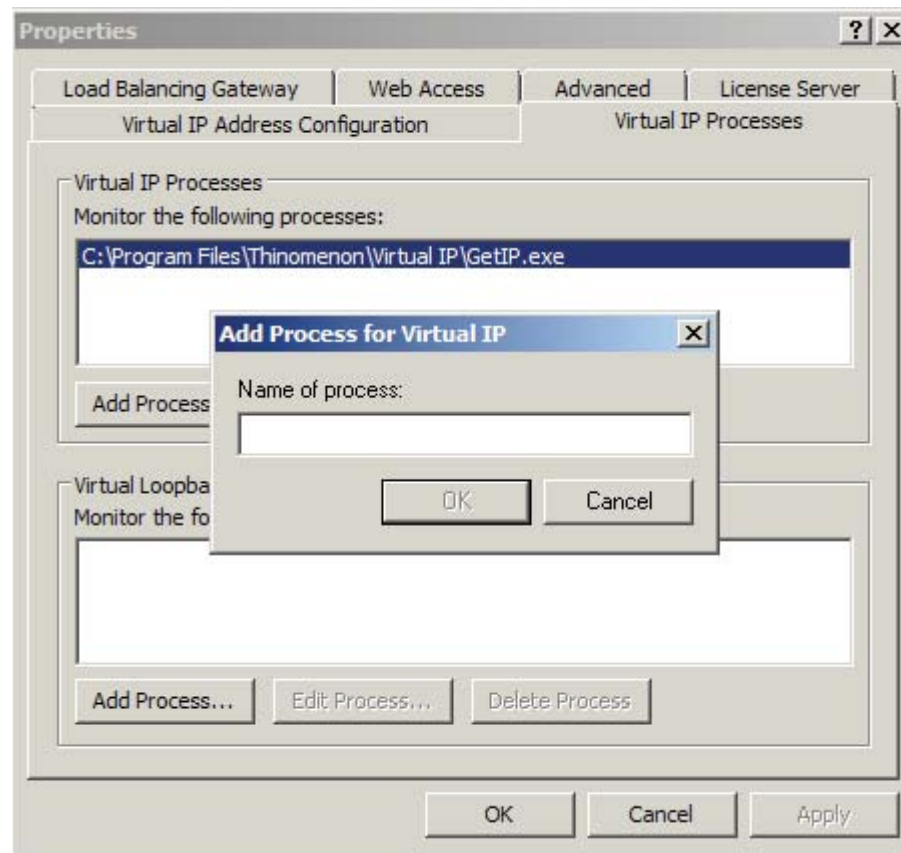
On the **Virtual IP Processes** tab you can specify processes for which IP address will be virtualized. These processes could belong to two groups: IP and Loopback processes.

To add process for monitoring:

1. Click the **Add Process...** on the **Virtual IP Processes** tab



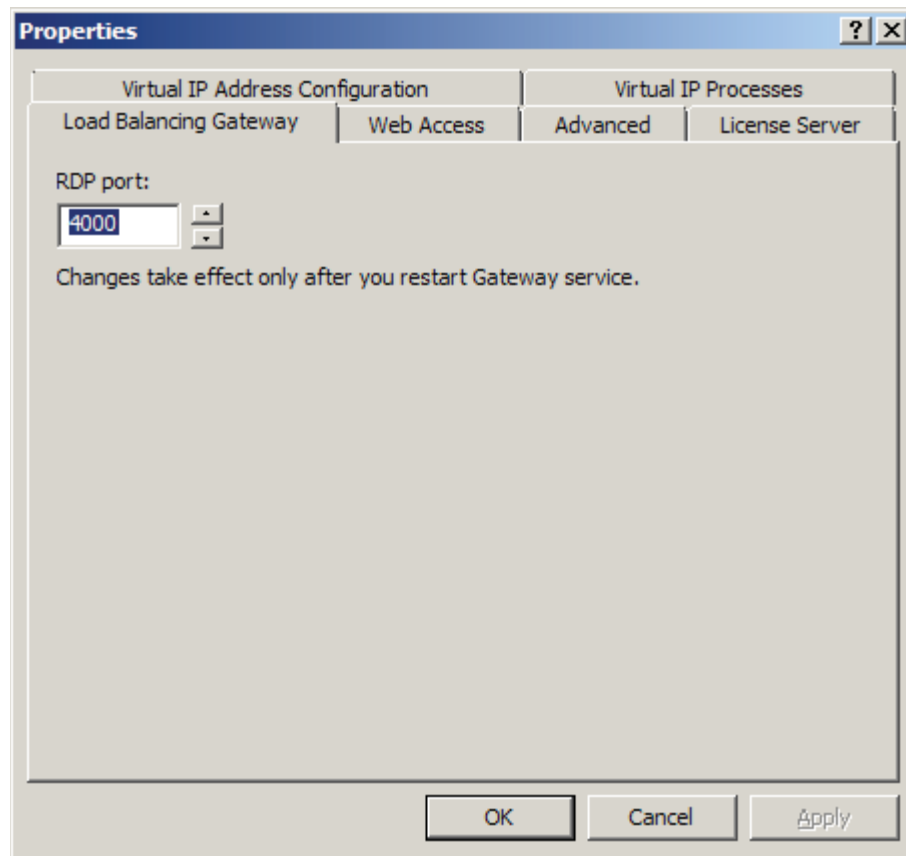
2. Enter the process name. Click **OK**.



3.1.3 Change a Port for Load Balancing Gateway

To change a port for Load Balancing Gateway:

1. Open Farm-wide settings
2. On the **Load Balancing Gateway** tab define the listening port for Load Balancer. The default port is TCP 4000. Click **OK**



3.1.4 Managing Web Access

3.1.4.1 Enable Web Access

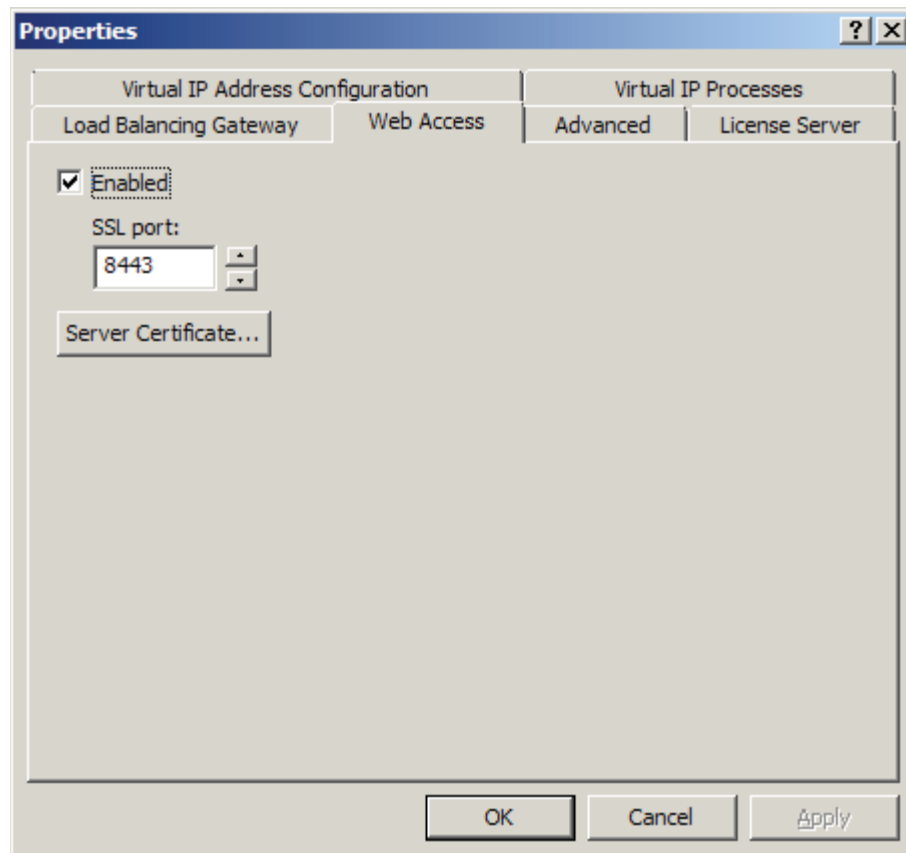
To enable Web Access:

1. Open Farm-wide settings
2. On Web Access tab check Enable checkbox. Click **OK**

3.1.4.2 Change a Port for Web Access

To change a port for Web Access:

1. Open Farm-wide settings
2. On Web Access tab define the SSL port for Web Client.



To generate a certificate request and/or import a certificate, click the ***Server Certificate***.

3.1.4.3 Certificate Installation.

SSL functionality relies on the server having a special certificate. This allows clients to validate the connection end-point and to generate a secure encryption key.

An administrator must first create a certificate request.

To generate a certificate request:

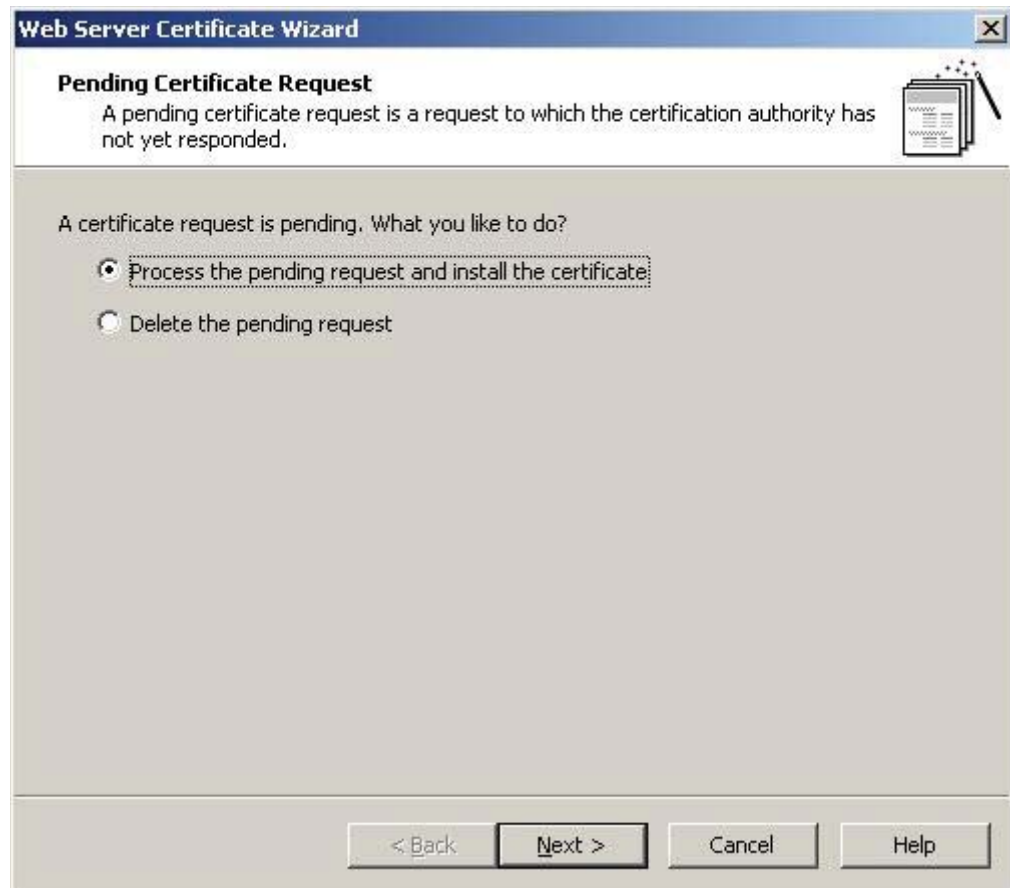
1. Launch *Enterprise Management Console*.
2. Select Farm node properties.
3. Go to *Web Access* tab. Click *Server Certificate*. Web Server Certificate wizard appears.



4. Specify necessary information and create request-file.

To enter the SSL certificate:

1. Launch *Enterprise Management Console*.
2. Select Farm-node Properties.
3. Go to *Web Access* tab. Click *Server Certificate*. Web Server Certificate wizard appears
4. Choose **Process the pending request and install the certificate**.



5. Specify path to the SSL certificate. Click *Next*

4. Click ***Finish*** to complete the certificate installation.

If you are unable to order certificates from an authority, see *Troubleshooting* -> *Creation of self-signed certificate with help of Thinomenon Certificate Tool* section to learn how to generate self-signed certificates.

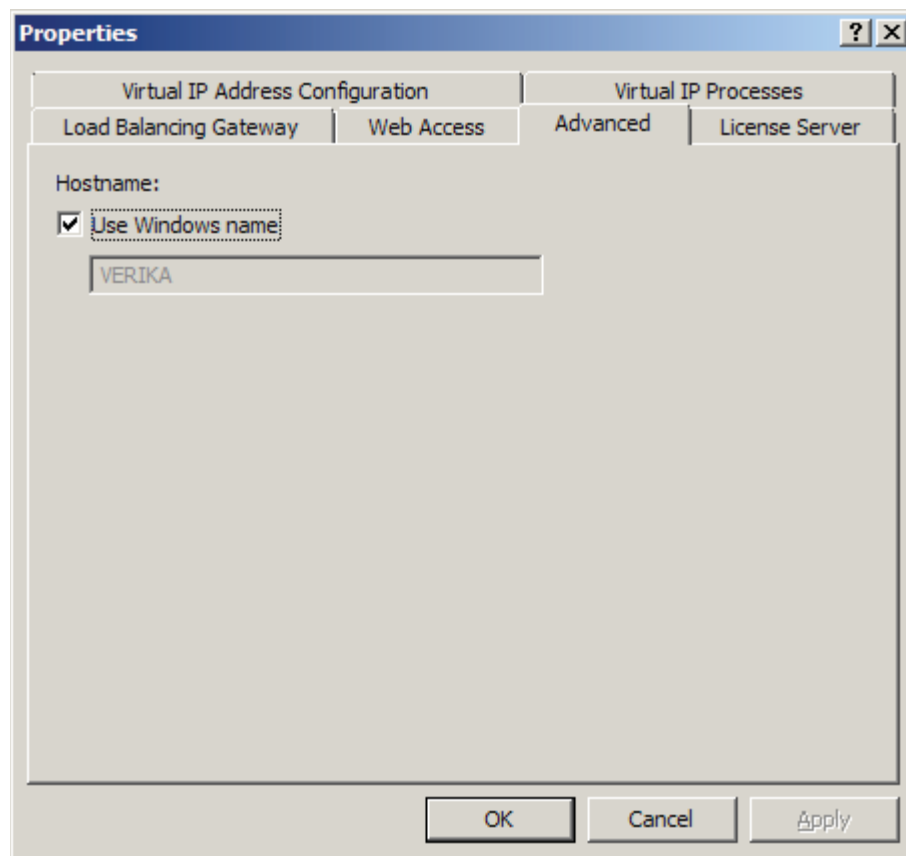
3.1.5 Change Host Name

On the **Advanced** tab of Farm Properties you can define the hostname used for generating RDP files from the Management Console.

By default, the Windows name of the computer host where Load Balancer is installed⁵ is used.

To edit the hostname value:

1. Select Farm-node Properties.
2. On Advanced tab uncheck the **Use Windows name** option and enter a required name in the field. Click **OK**.



⁵ In All In One setup, no Load Balancer is needed and hostname of the single server is used.

3.1.6 Specify License Server

On the **License Server** tab, specify the hostname of License Server.

If License Server is installed together with Enterprise Management Console, the Windows name of the computer host is used for the License Server. Otherwise, you need to manually enter License Server computer name/address.

This information is required for automatic Guest Tools installation.

To enter the License Server information:

1. Select Farm-node Properties
2. From the License Server tab, enter the License Server information.

Properties [?] [X]

Virtual IP Address Configuration | Virtual IP Processes

Load Balancing Gateway | Web Access | Advanced | **License Server**

Enter the host name or the Internet Protocol (IP) address of the computer where the License Server is installed.

For example, 192.168.0.1 or myserver.local.

License Server:

3.2 Managing Published Items

Thinomenon Access Suite 2.0 allows publishing:

Applications,

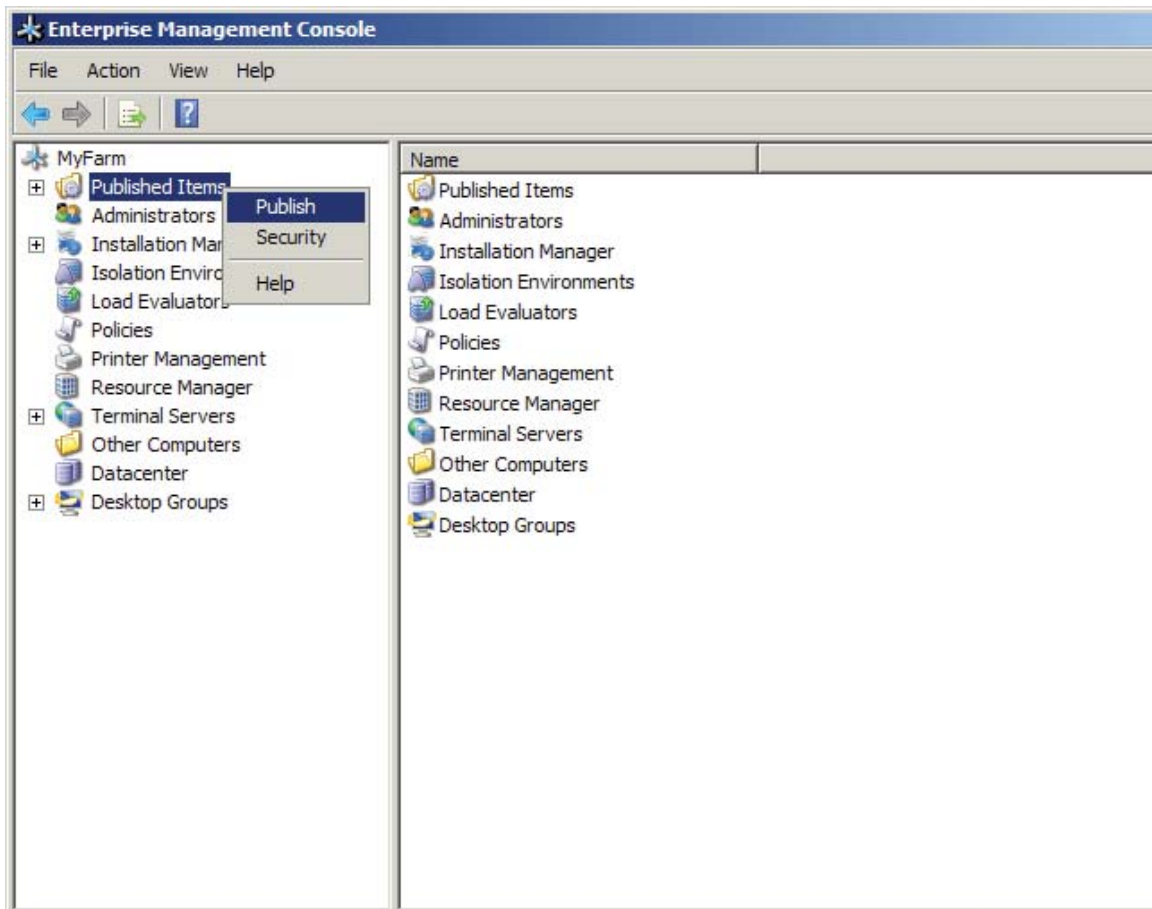
Desktops,

Documents.

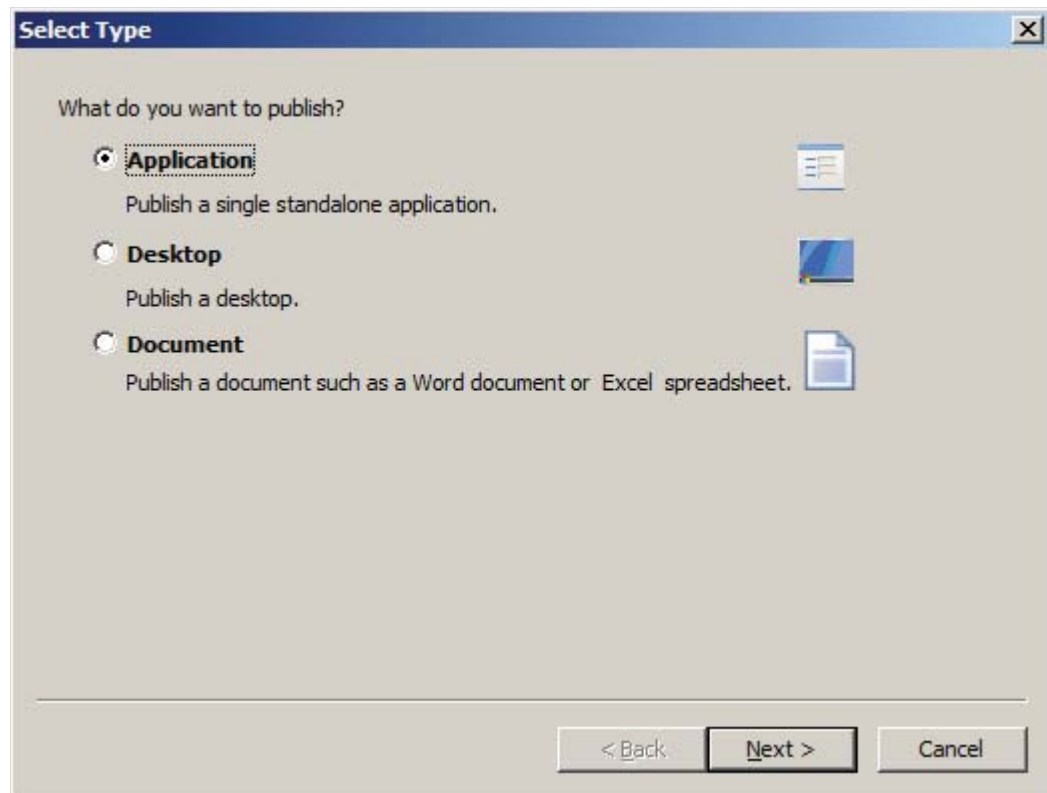
The procedure of item publishing differs depending on the item type.

To publish the item:

1. Right-click the ***Published Items*** node and select ***Publish*** or select ***Action-> Publish***.

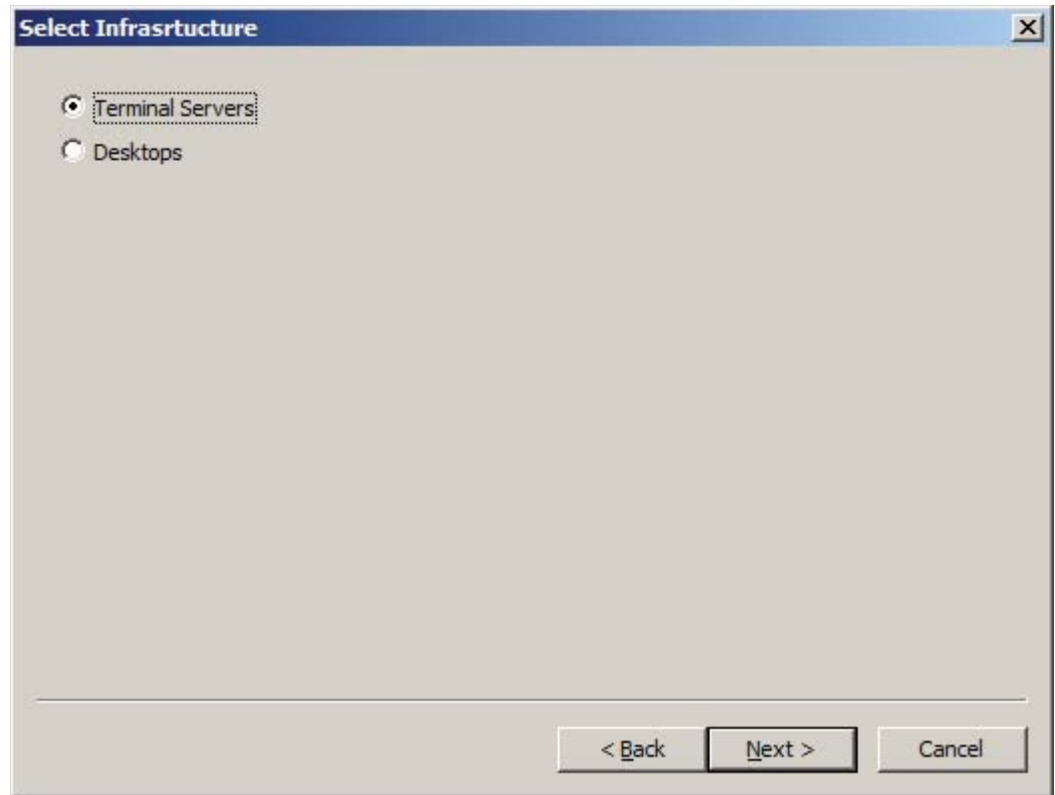


2. Select the type of the item to be published (Application, Desktop or Document). Click ***Next***.



3. On the next page select *Terminal Servers* or *Desktops* as a back-end then click *Next*.

If you select Terminal Servers and to use load balanced servers, first create Load Evaluators.

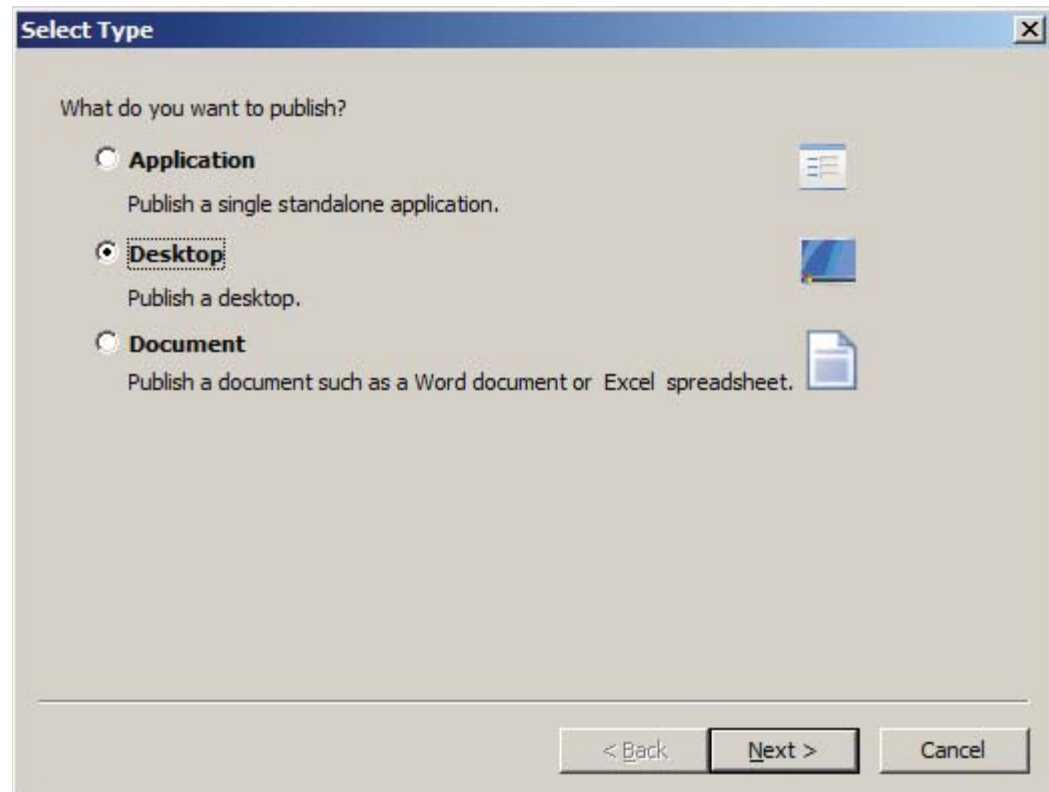


4. Next steps depend on the type of the item being published.

3.2.1 Publishing Desktop

To publish a full desktop:

1. Select the **Desktop** as a type of the item being published on the **Select Type** page of the wizard and click **Next**.



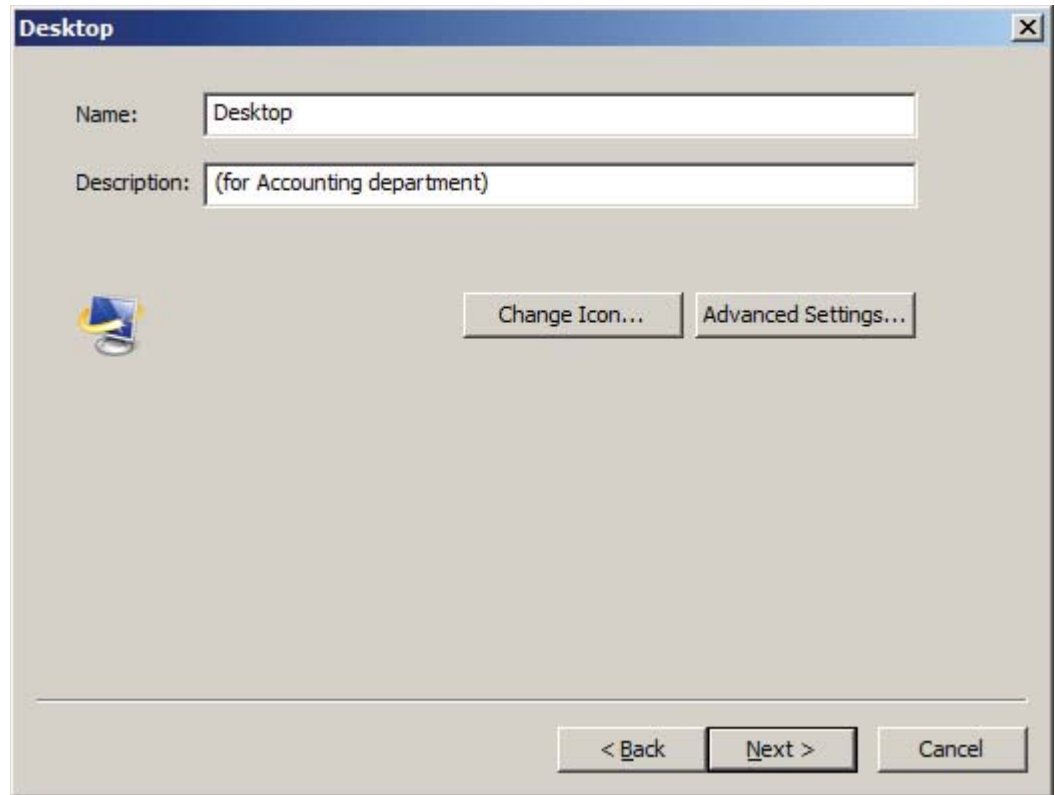
2. Select back-end infrastructure (Terminal Servers or Desktops)
3. On the next page, enter information about a desktop and click **Next**:

Name: The desktop name. This name will be displayed in Management Console and on Client.

Description: The description for the desktop if necessary.

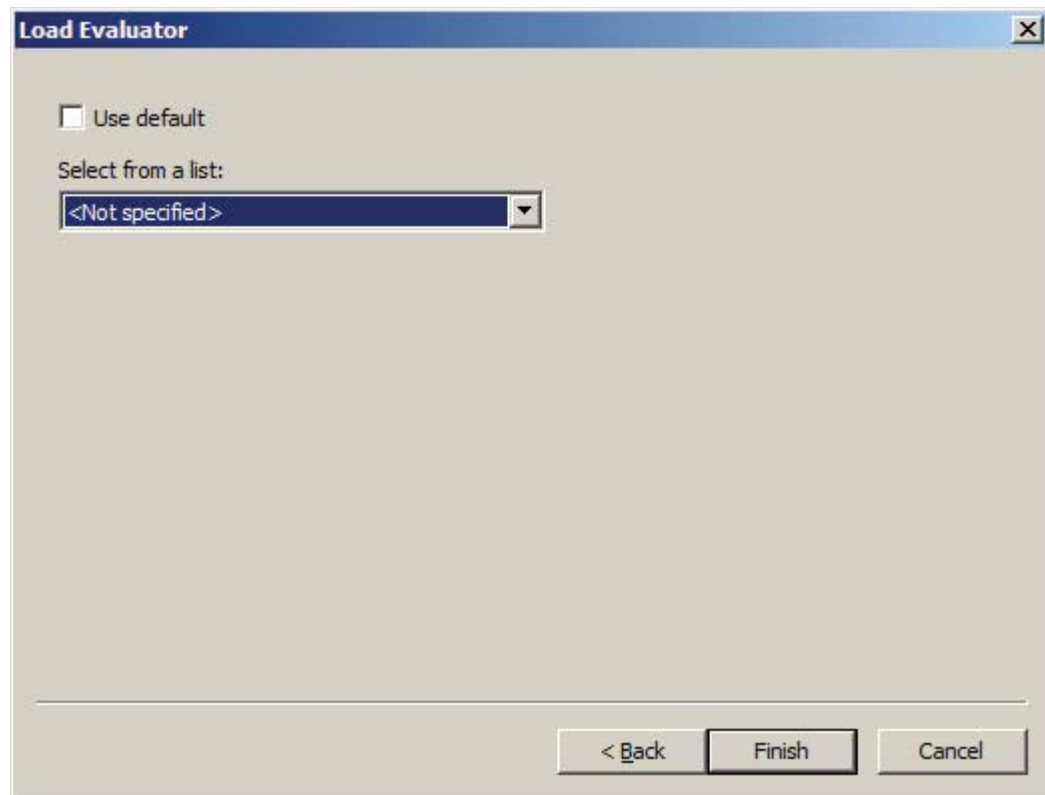
Change Icon: Change default icon of your desktop to some custom icon.

Advanced Settings: Server-side adjustments for published desktop. These settings will be applied to desktops launched from Web Portal.



4. Configure filtering settings and click *Next*. Define which users and/or groups of users will have an access to this published desktop, associate the published desktop with the specific Terminal Servers/Desktop groups or computers with specific operating system. For more details, please address the *Filtering* section described below.

5. On the Load Evaluator page, select the load evaluator. Use the default load evaluator or choose one from the drop-down list. To be able to do it, create load evaluators first.



3.2.2 Publishing the Application

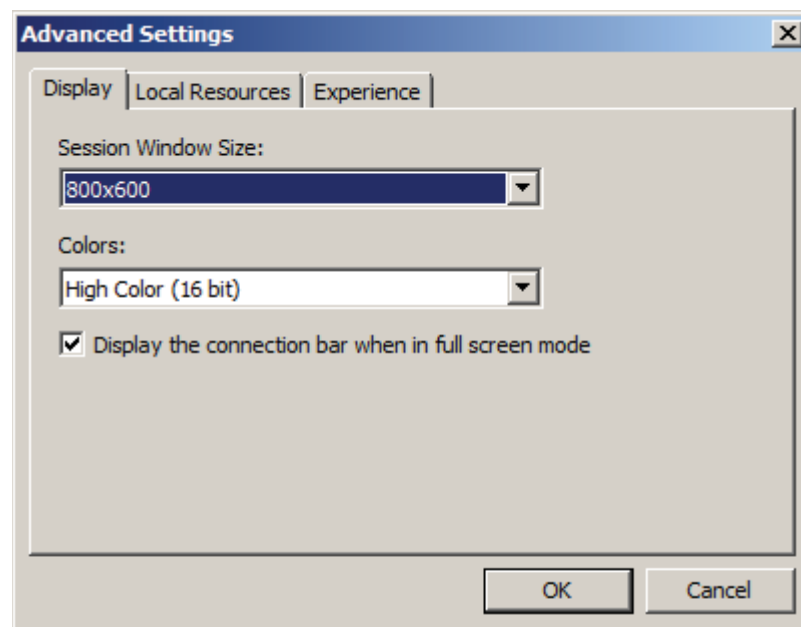
1. Select Application as the type of the published resource.
2. On the next page, enter information about the application. Click **Next**.
 - Name: The application name. This name will be displayed in Management Console and on Client.
 - Description: The application description if necessary.
 - Run: Size of application window (Normal, Maximized, and Minimized).
 - Location: Terminal Server or Desktop Group for **Target** browse dialog to be opened.
 - Machine: (for Desktops infrastructure only) virtual machine, which belongs to Desktop Group specified in **Location** field; **Target** browse dialog will be opened from this machine.
 - Target: The path to the application executable file (you can enter the path manually)
 - Start in: Full path to the application folder (application will be started within this folder).
 - Parameters: If necessary, application can be published with parameters. For example, to publish some batch file (*.bat) you need to publish the CMD application and specify /C and the path to the batch file as an argument as shown on the screenshot.

The screenshot shows the 'Application' dialog box with the following fields and values:

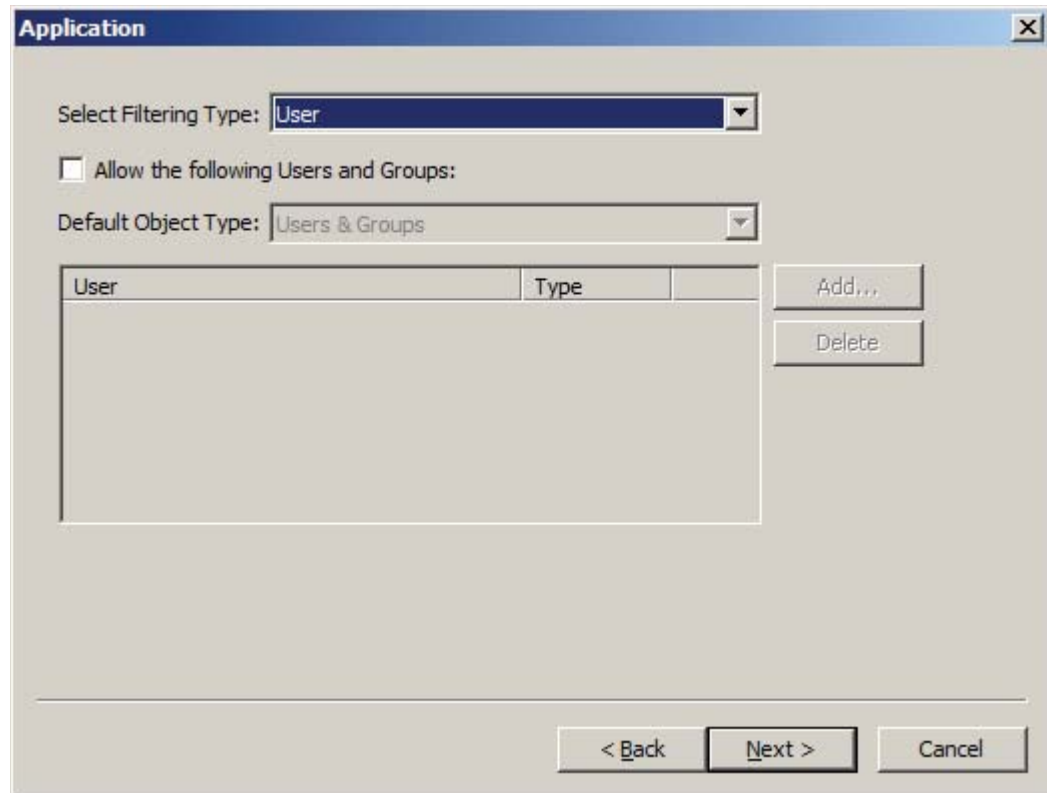
- Name:** cmd
- Description:** (empty)
- Run:** Normal Window
- Location:** VERIKA
- Target:** C:\Windows\System32\cmd.exe
- Start in:** C:\Windows\System32\
- Parameters:** /C C:\bat.bat

Buttons at the bottom: OK, Cancel, Apply.

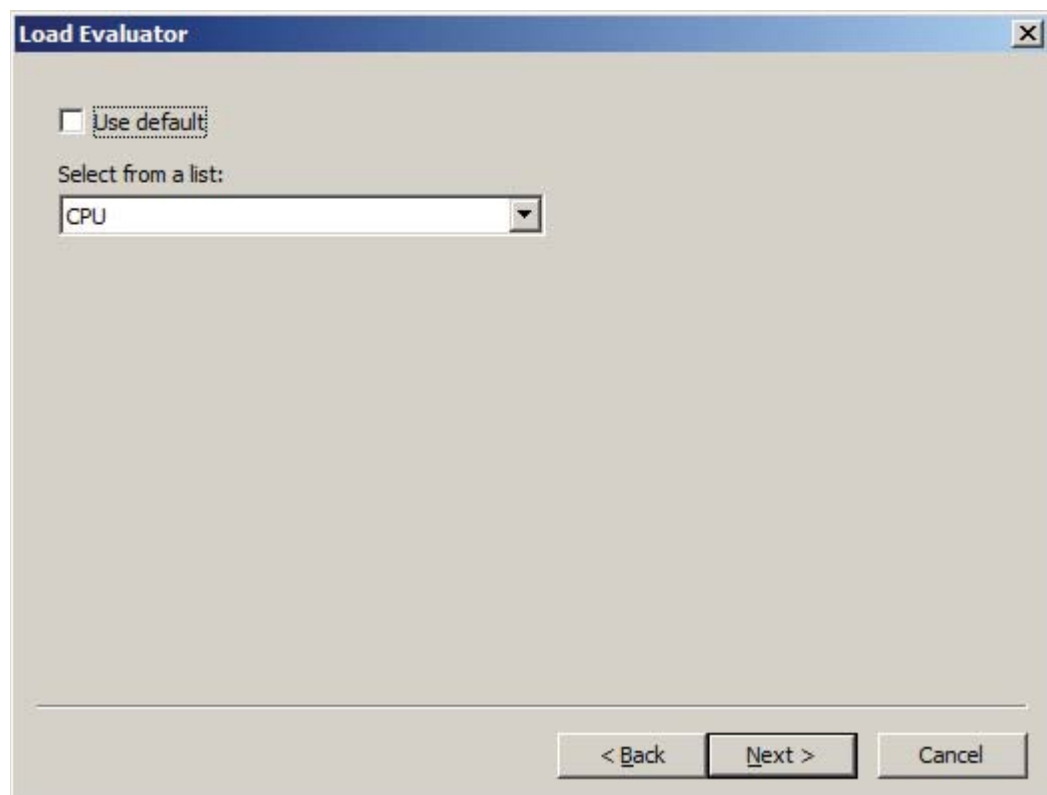
- Change Icon: Change default icon of your application to some custom icon.
- Advanced Settings: Server-side adjustments for published application. These settings will be applied to applications launched from Web Portal. These settings include...
- Display: TBD
- Local Resources: TBD
- Experience: TBD



3. Configure filtering and click *Next*. Define which users and/or groups of users will have access to this published application, to tie published item to specific Terminal Servers/Desktop groups or to computers with specific operating system. For more details please address *Filtering* section described below.



3. Select Load Evaluator. Use the default load evaluator or choose one from the drop-down list.



4. Configure *Associate File Extensions* and *Allow only one instance* features.

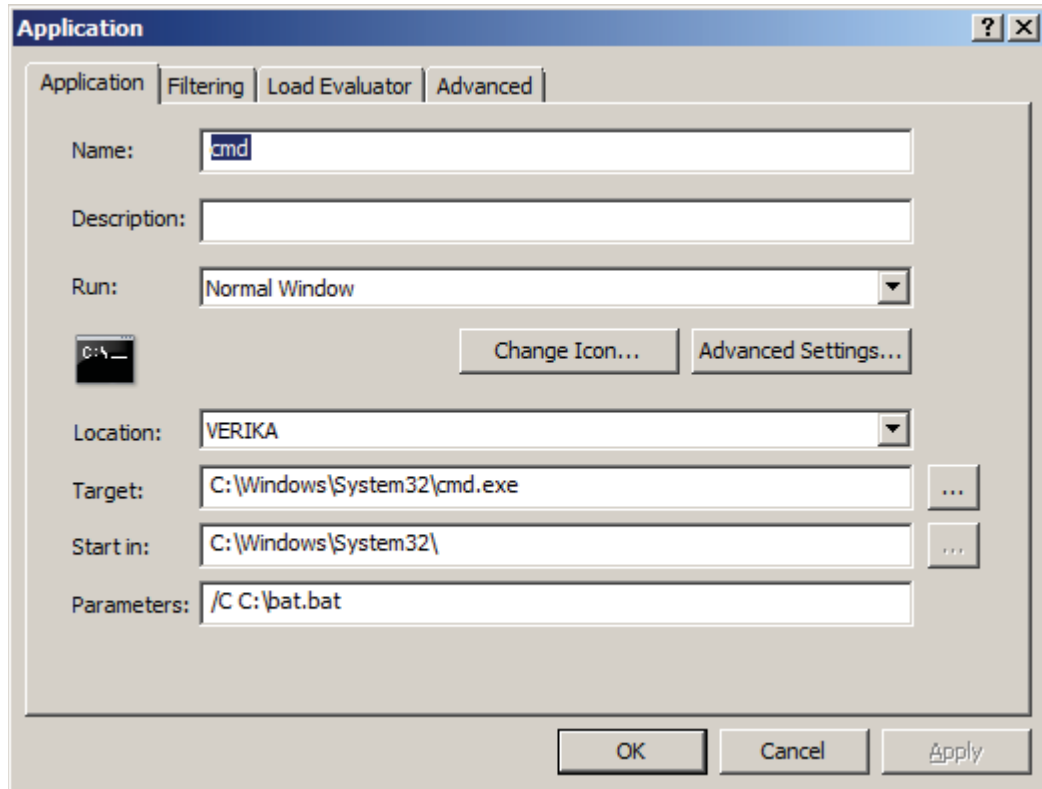
- The ***Associate File Extensions*** feature allows associating specific file extensions with the published application, so that end-users could open local files using published applications. Please note that the ***Associate File Extensions*** feature must be enabled from Enterprise Management Console and also from Access Client on the client-side.
- The ***Allow only one instance*** option limits the number of instances of the application which can be launched by the same user within a single session. If selected, users will be allowed only one instance of application launched¹.

¹ Work of this option on Terminal Server also depends on state of ***Restrict each user to a single session*** option, which is configured in Terminal Server's properties. For more details see Appendix C.

3.2.2.1 Modifying Published Application Settings

To modify published application settings:

1. Right-click the ***Published Application*** and select ***Properties***.
2. Application settings Window Appears.



3. Once changes are made, click ***OK***.

3.2.2.2 Managing File Extensions

To manage File Extensions you need to enable Association File Extensions for Application

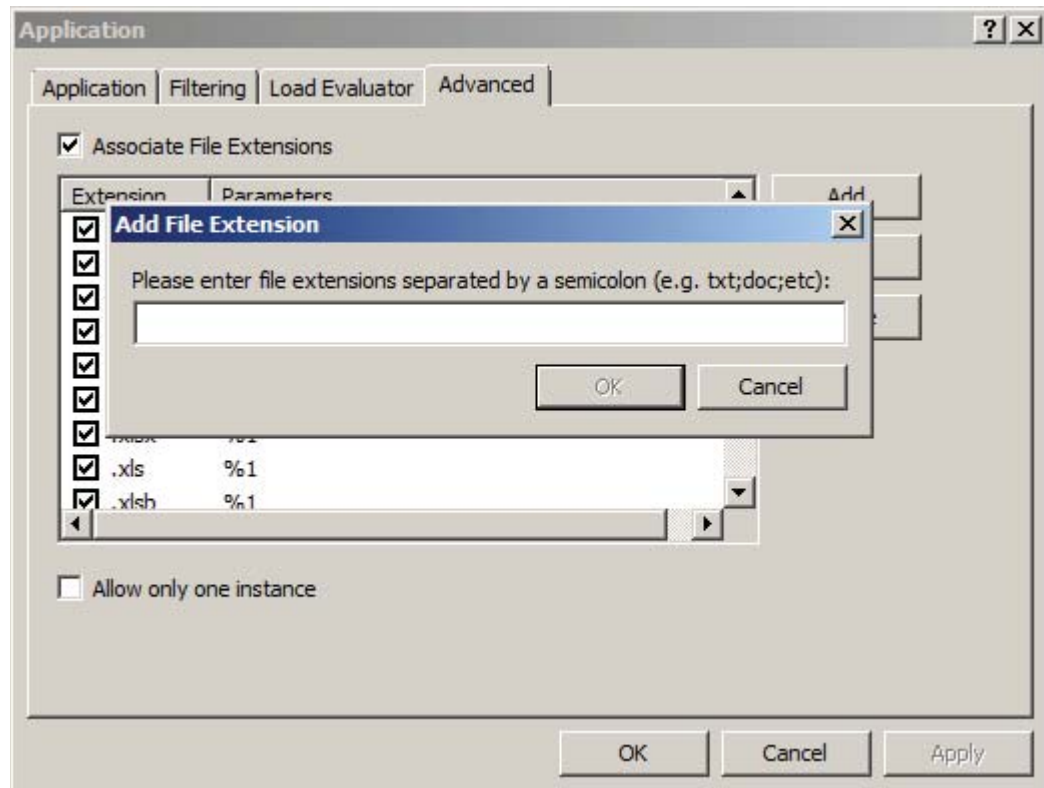
To enable Association:

1. Right-click the ***Published Application*** and select ***Properties***.
2. Go to ***Advanced*** tab.
3. Check Associate File Extensions option.

3.2.2.2.1 Add File Extensions

To add File Extension:

1. Right-click the ***Published Application*** and select ***Properties***.
2. Go to ***Advanced*** tab.
3. Click ***Add***. Add File Extension window appears.



4. Enter file extension(s). Click **OK**.

3.2.2.2.2 Edit File Extensions

To Edit File Extensions:

1. Right-click the **Published Application** and select **Properties**.
2. Go to **Advanced** tab.
3. Select created Extension.
4. Click **Edit**. Edit parameters window appears.



5. After you make changes click **OK**

3.2.2.2.3 Delete File Extensions

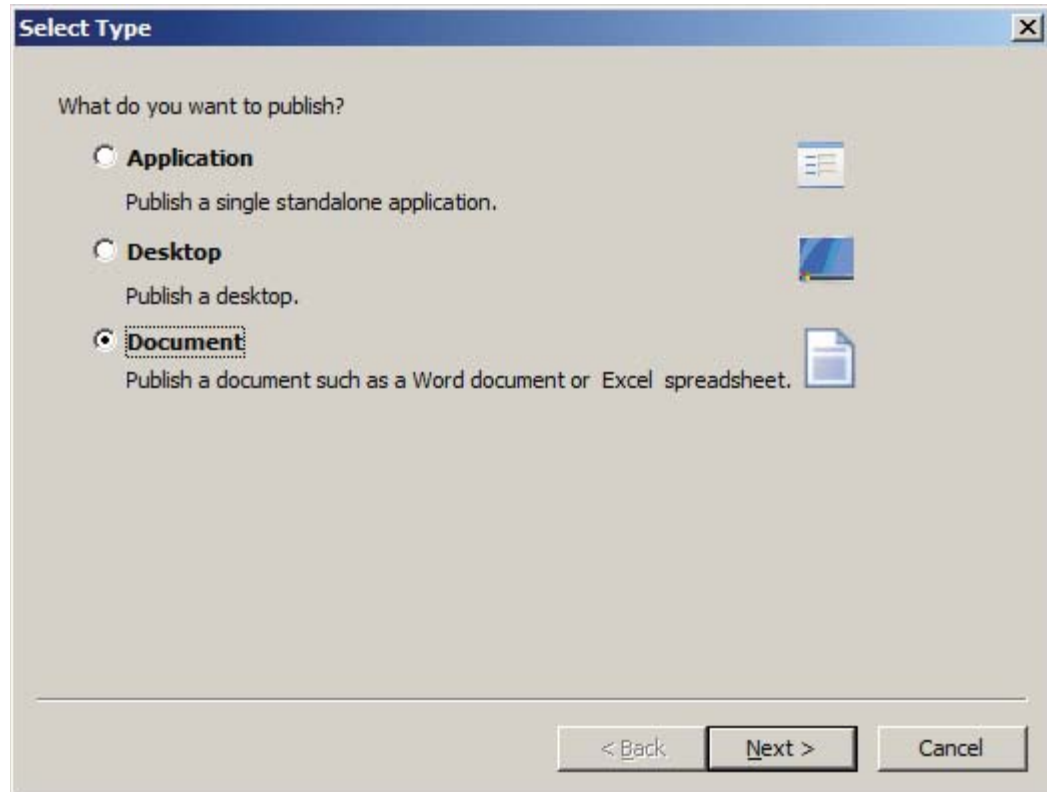
To Delete File Extensions:

1. Right-click the **Published Application** and select **Properties**.
2. Go to **Advanced** tab.
3. Select created Extension.. Click **Delete**.

3.2.3 Publish Document

To publish a document:

1. On the **Select Type** page of the publishing wizard, choose **Document** and click **Next**.



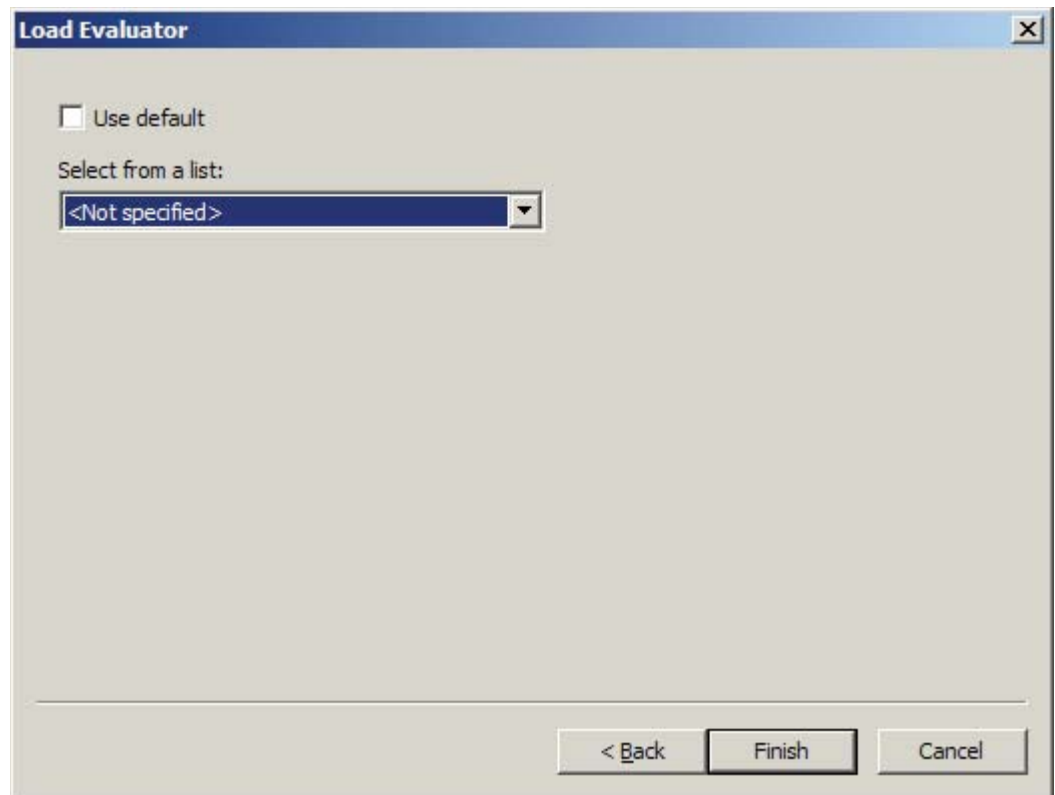
2. Select the infrastructure (Terminal Servers or Desktops)
3. On the next page define the following settings and click **Next**:
 - Name: The document name. This name will be displayed in Management Console and on Client.
 - Description: The document description if necessary.
 - Location: Terminal Server or Desktop Group for **Content** browse dialog to be opened.
 - Machine: (for Desktops infrastructure only) virtual machine belonging to Desktop Group specified in **Location** field; the **Content** browse dialog will be opened from this machine.
 - Content: Browse the document (you can enter the path manually)
 - Change Icon: Change default icon of your document to some custom icon.
 - Advanced Settings: Server-side adjustments for published document. These settings will be applied to documents launched from Web Portal.

The screenshot shows a 'Document' dialog box with the following fields and controls:

- Name:** Price list
- Description:** (empty text box)
- Location:** VERIKA (dropdown menu)
- Content:** C:\Price list.xlsx (text box with a browse button '...')
- Buttons:** Change Icon..., Advanced Settings..., < Back, Next > (highlighted), Cancel

4. Configure filtering: define which users and/or groups of users will have an access to this published desktop, associate the published desktop with the specific Terminal Servers/Desktop groups or computers with specific operating system. For more details, please address the **Filtering** section described below.

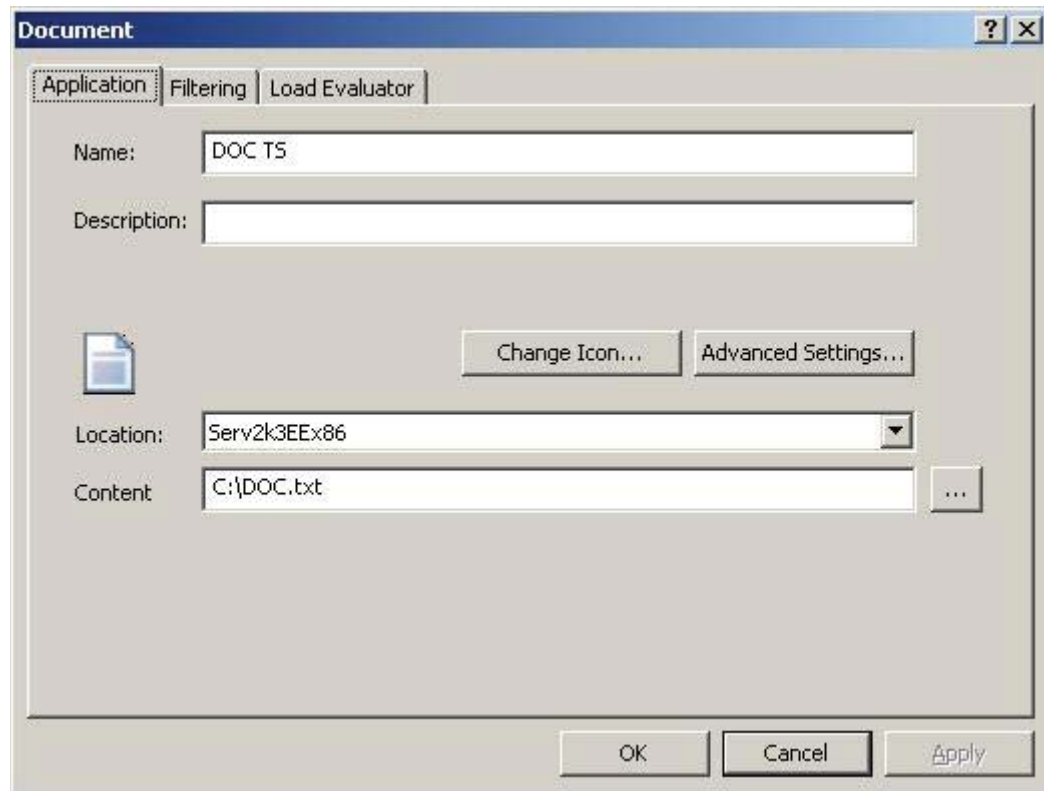
5. On the Load Evaluator page, select load evaluator. Use the default load evaluator or select one from the drop-down list.



3.2.3.1 Modifying Published Document Settings

To modify published Document settings:

1. Right-click the **Published Document** and select **Properties**.
2. Document settings Window Appears.



3. To modify Advanced Settings click **Advanced Settings** Button.
4. After you make changes click **OK**.

3.2.4 Delete Published Items

To delete published items:

1. Right-click the **Published Item** and select **Delete**. **Confirmation Window** appears.
2. Click **Yes** if you are sure you want to delete this item.

3.2.5 Managing Filtration for Published items

Filtering is defined for each published item and determines whether this published item can be launched by the current user in the current environment.

There are three types of filters:

- filtering by users;
- filtering by servers (Terminal servers infrastructure)/groups (Desktops infrastructure);
- filtering by operating systems.

The filtering settings can be defined when the item is published and changed in its Properties any time in future.

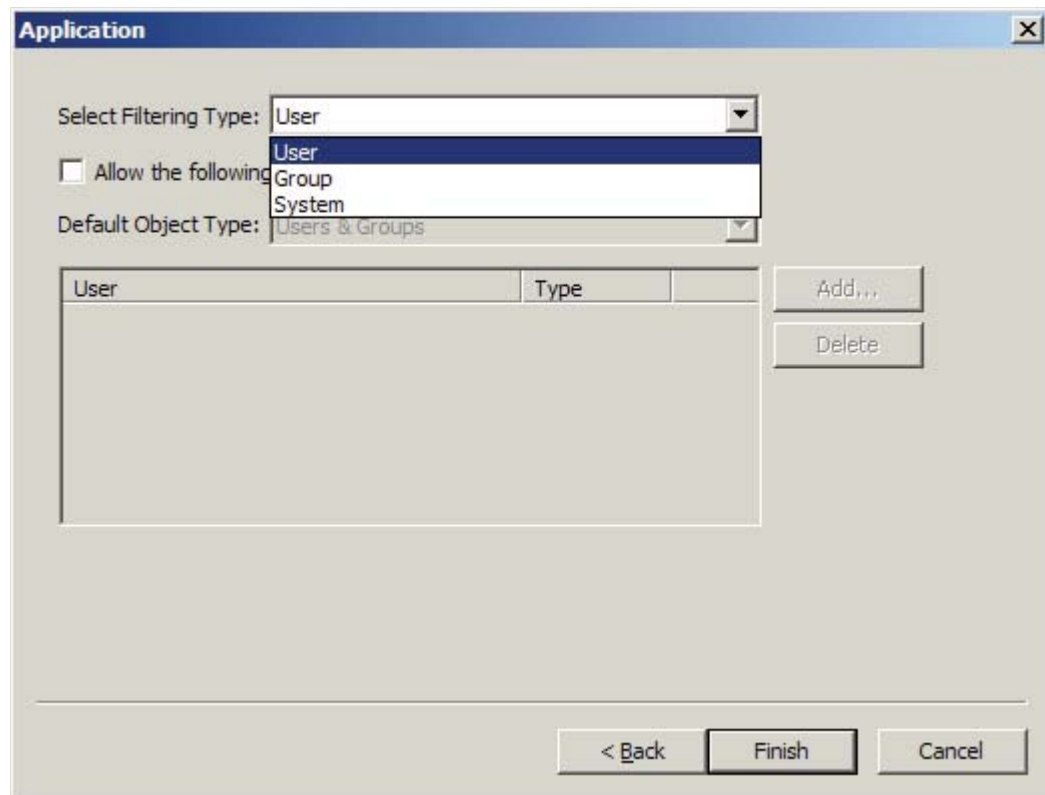
To change filtering settings:

1. Right-click the Published item and select Properties.
2. In the Properties window, select the ***Filtering*** tab.

3.2.5.1 Filtering by User

Filtering by users

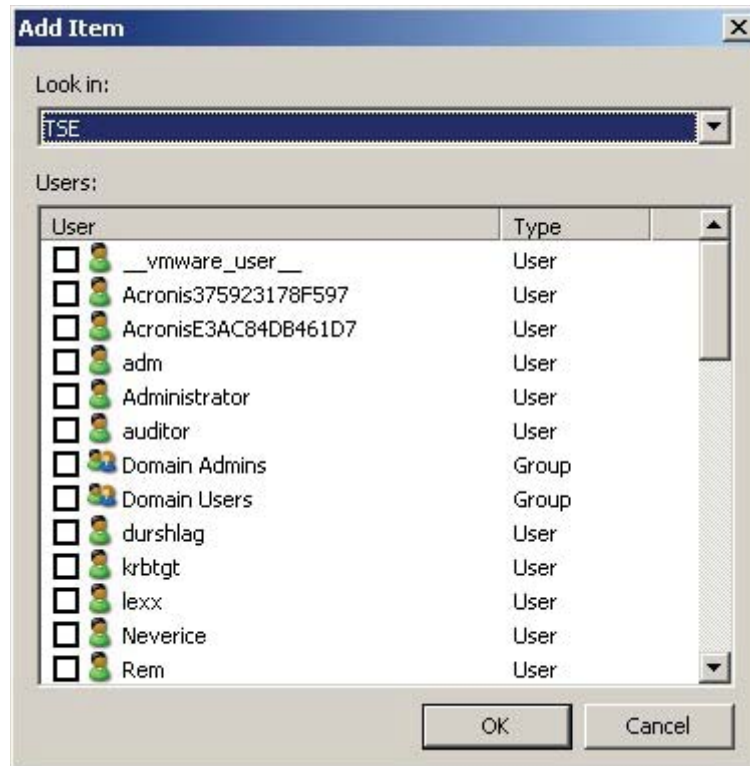
1. Open the ***Filtering*** tab of published item properties and select ***User*** as Filtering type.



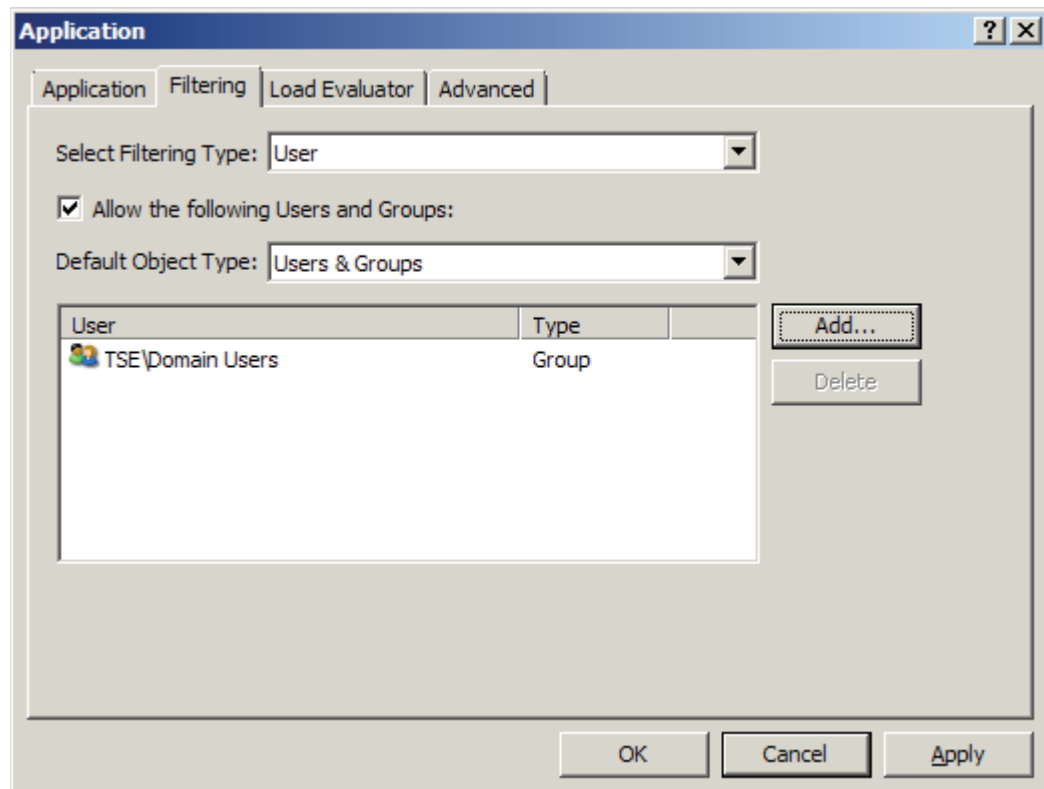
2. Check the *Allow the following Users and Groups* checkbox, and click *Add*.
3. The *Add Item* dialog opens.
4. In the *Look In* item drop down list choose destination from where the users will be selected.

NOTE: The *Look in* drop down list differs a bit depending on infrastructure. If the item is being published from Terminal Servers, both domain users and groups of users, and local users and groups of users of Member Servers are available. For items published from Desktops, domain users and groups of users can be selected only. Only those users who have local access rights are present (by default, it's administrators and members of Remote Desktop Users group). Please address the *Appendix D* to see how to make users/groups be present in the Filtering list.

Select users and groups of users which will be allowed to launch this published item and click *OK*.



Please note users that are not added to the Filtering list will not see this published item from Client in published items list.



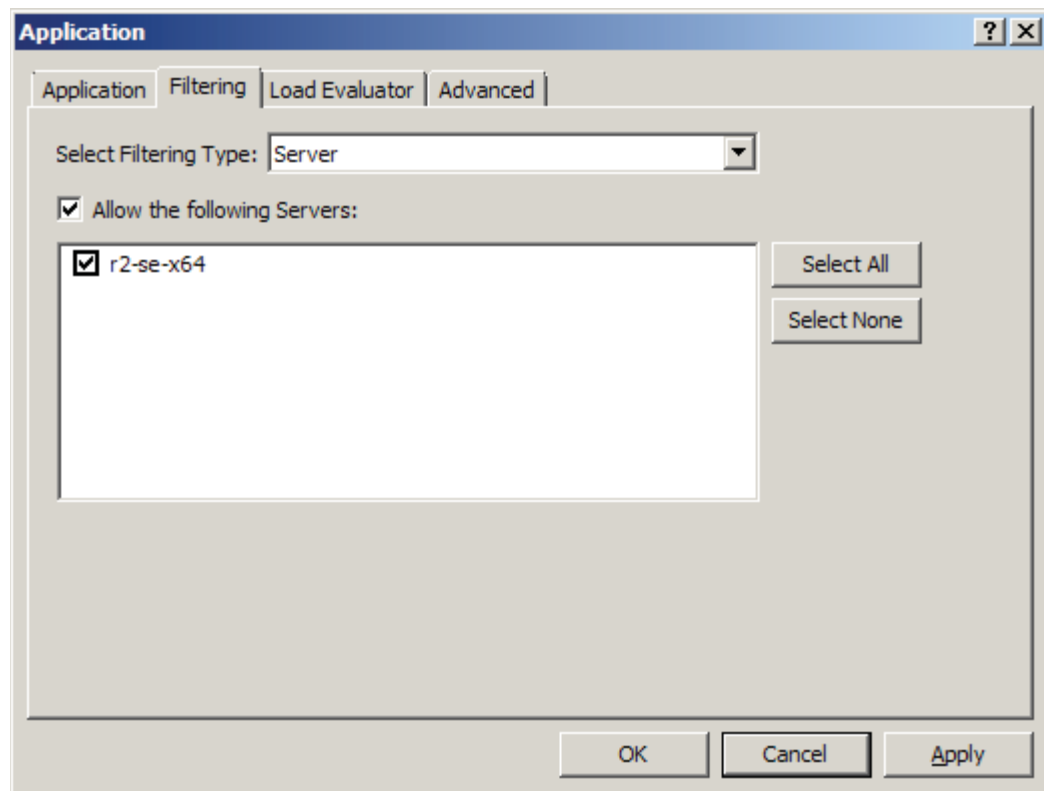
3.2.5.2 Filtering by Server (For Terminal Servers)

Filtering by servers/groups

Filtering by servers is available for Terminal Servers infrastructure, filtering by groups is meant for Desktops infrastructure.

To set filtering by Server:

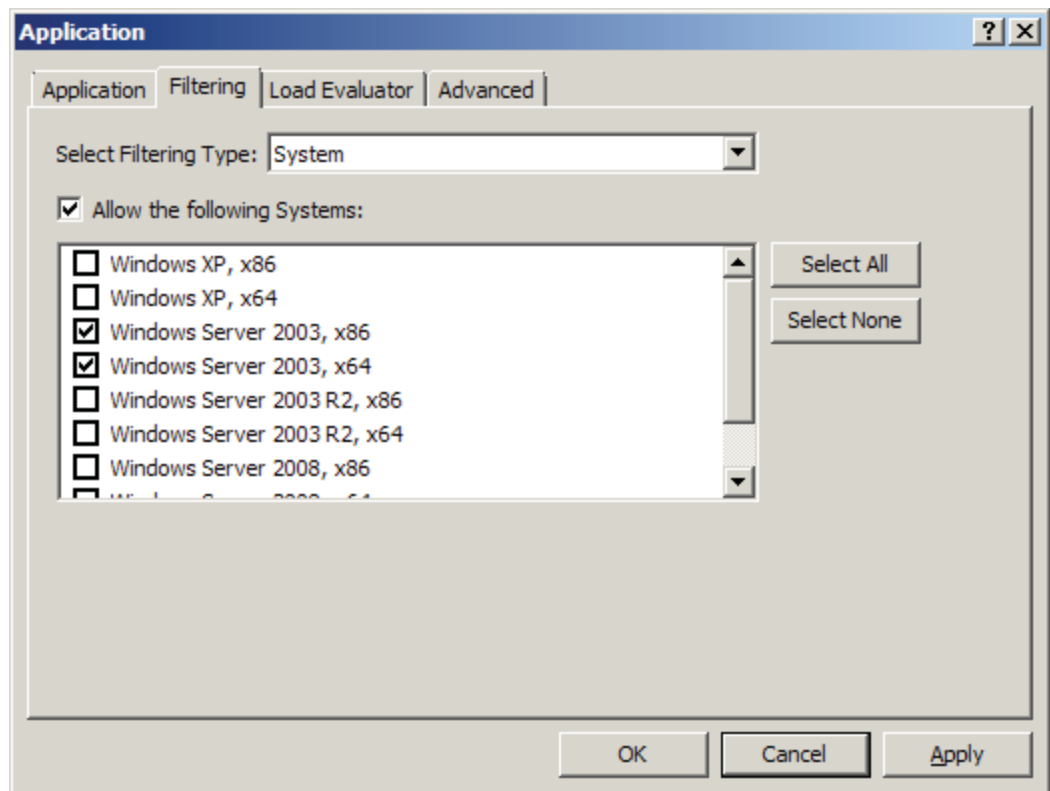
1. Open the **Filtering** tab of published item properties.
2. Select **Server** as Filtering type, and check the **Allow the following Servers** checkbox.
3. Select servers from the list of available Terminal Servers to allow published items launching from these servers.



3.2.5.3 Filtering by Systems

Filtering by operating systems allows you to assign the published item to computers running the specific operating system.

1. Open the **Filtering** tab of published item's properties.
2. Select **System** as Filtering type, and check the **Allow the following Systems** checkbox.
3. Select the operating systems you need from the list:

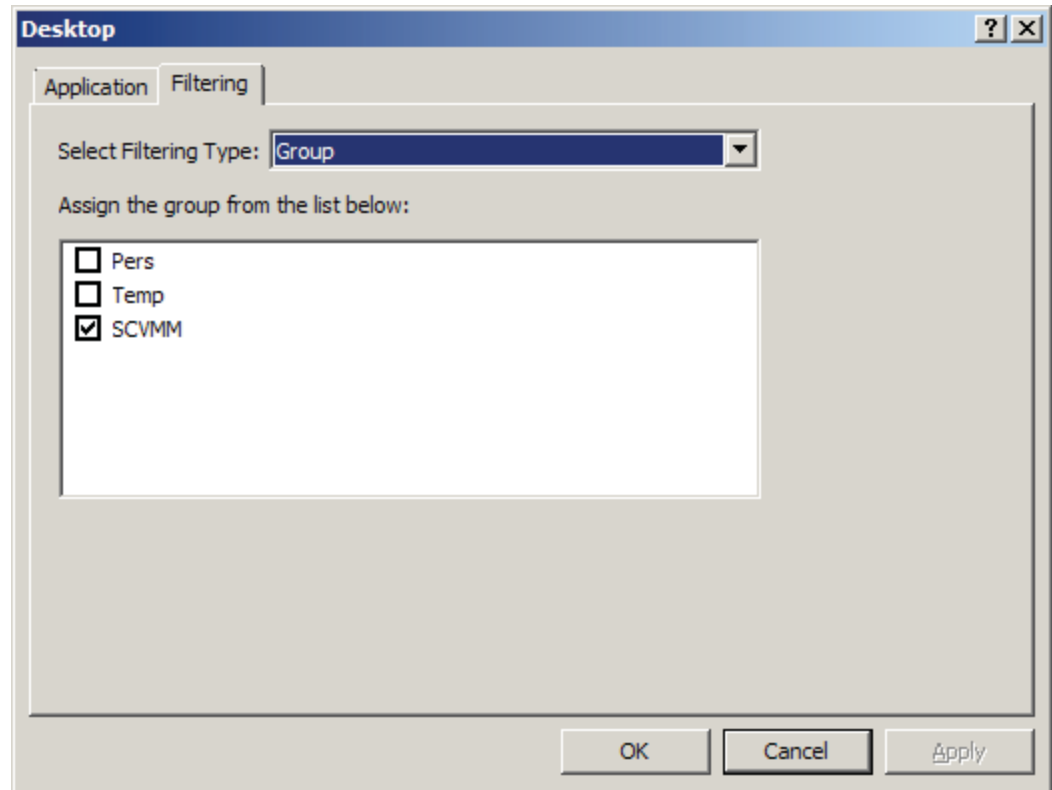


4. If filtering by operating system is set for certain published item, it won't be launched from the computer with improper operating system.

3.2.5.4 Filtering by Group

To set filtering by Group:

1. Open the **Filtering** tab of published item properties.
2. Select **Group** as Filtering type.
3. Select the Desktop group you want to launch published items from



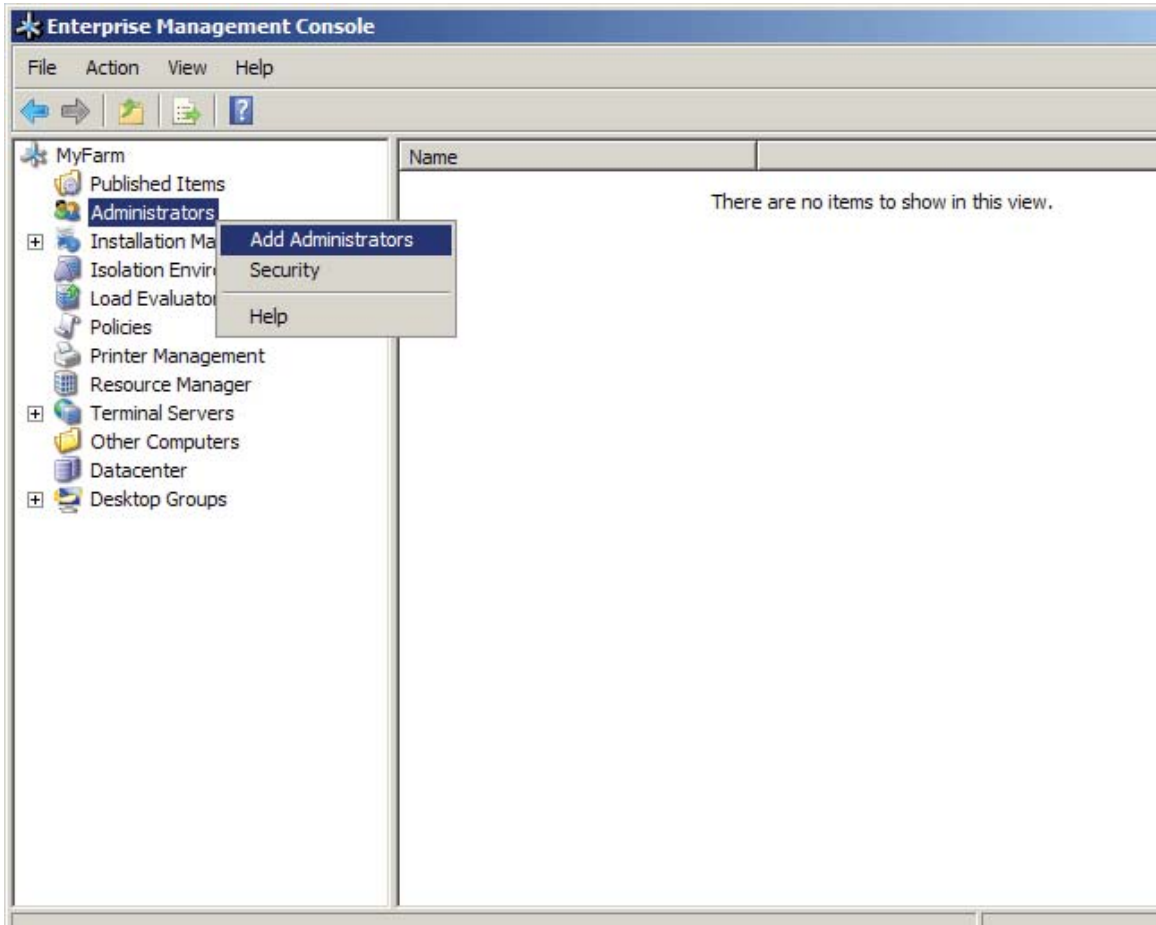
3.3 Managing Administrative Privileges

3.3.1 Adding Administrators

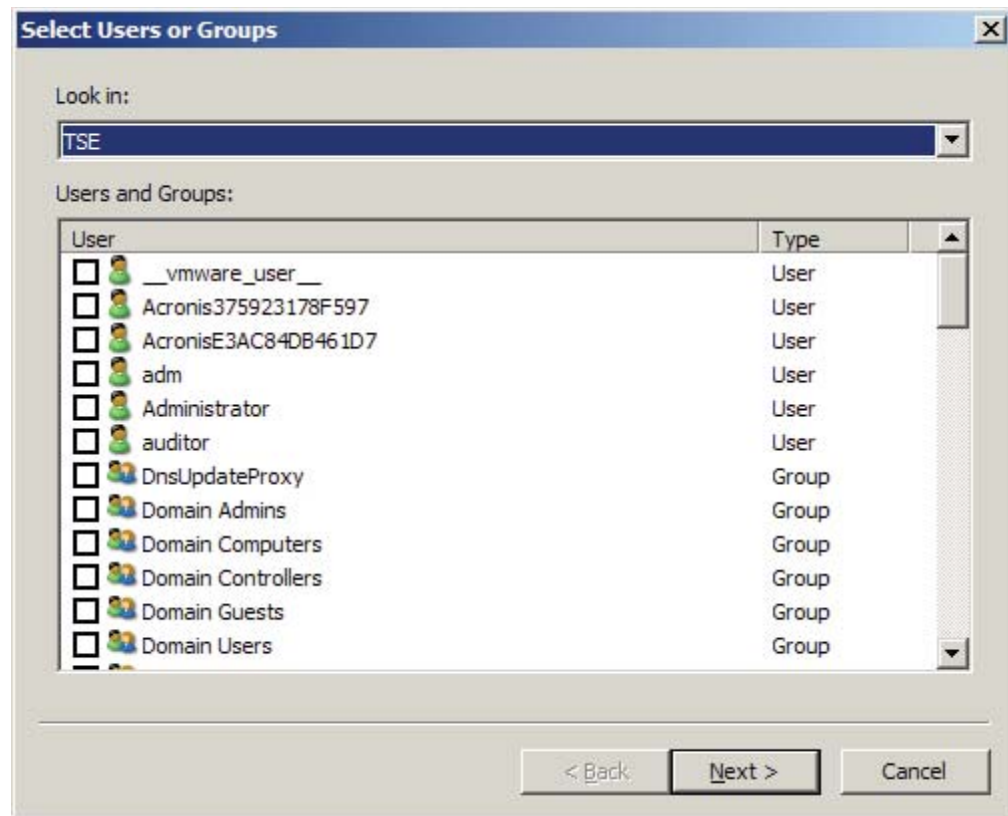
The Delegated Administration feature allows distributing administrative tasks among multiple levels of users.

To define administrators:

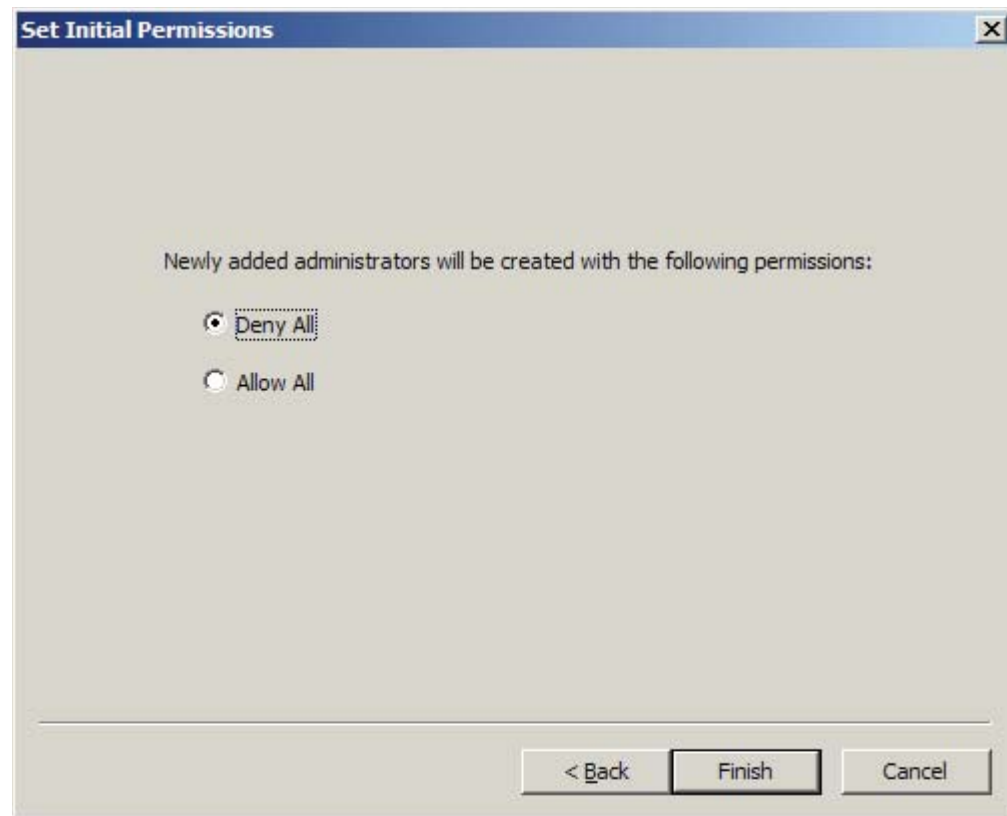
1. Right-click the *Administrators* node and select *Add Administrators*.



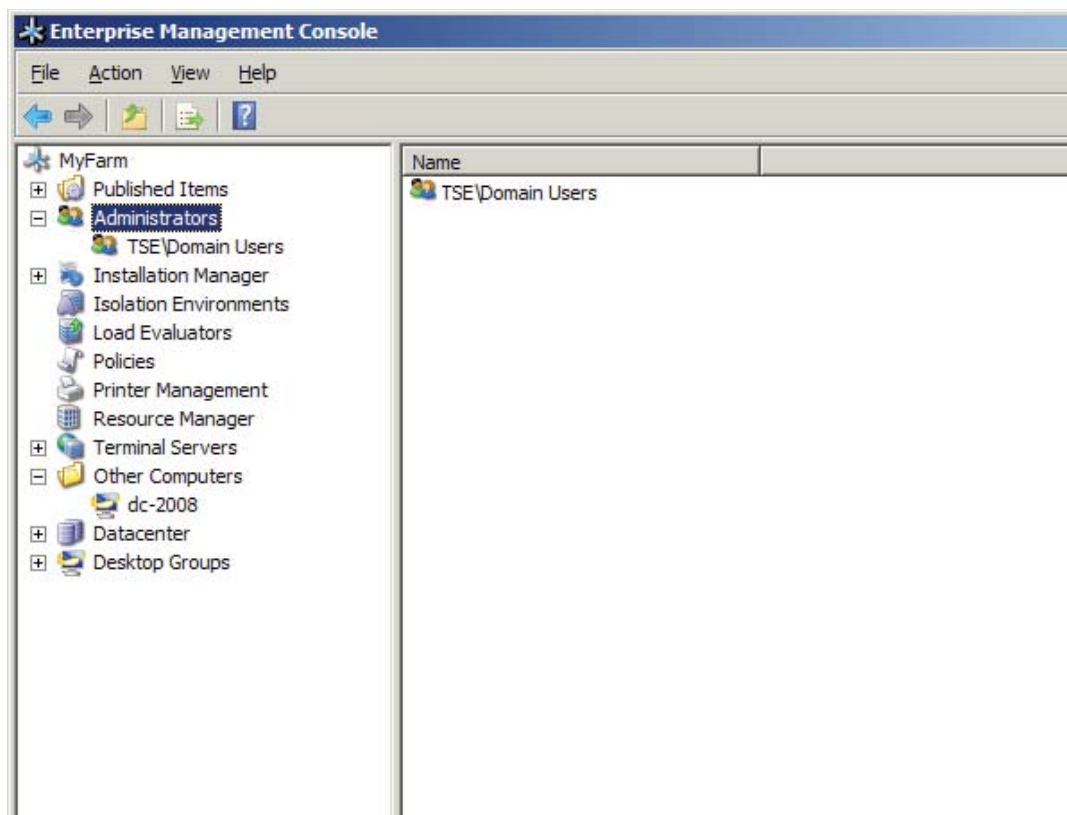
2. The *Select Users or Groups* Dialog opens.



3. Select users or group of users and click *Next*.
4. Select the set of initial permissions. Permissions allow or deny administrators actions within the Enterprise Management Console.



5. The added Administrator is displayed in Management Console tree.



3.3.2 Deleting Administrators

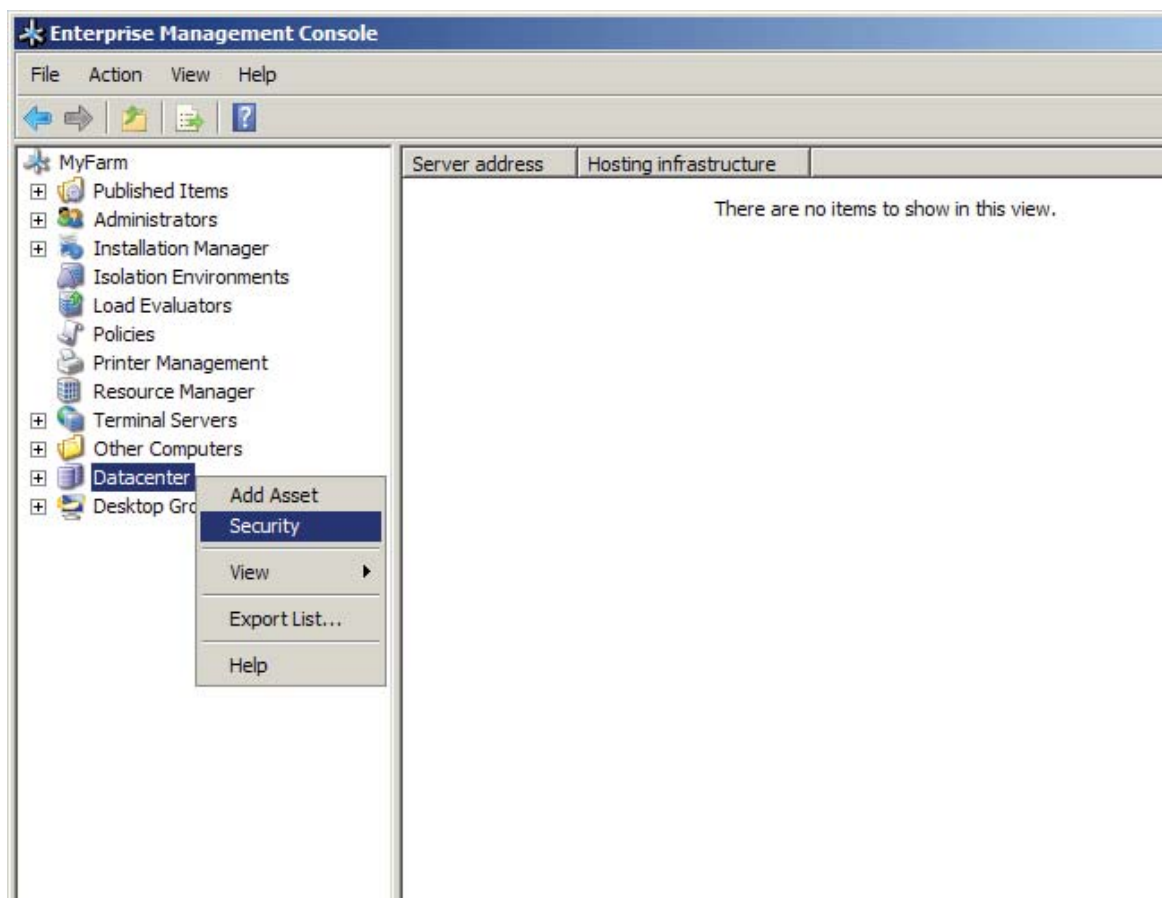
To delete Administrators:

1. Right-click the **Administrator** you want to remove and select **Delete**.
2. Confirmation Window appears.
3. Click **Yes** if you are sure you want to delete Administrator.

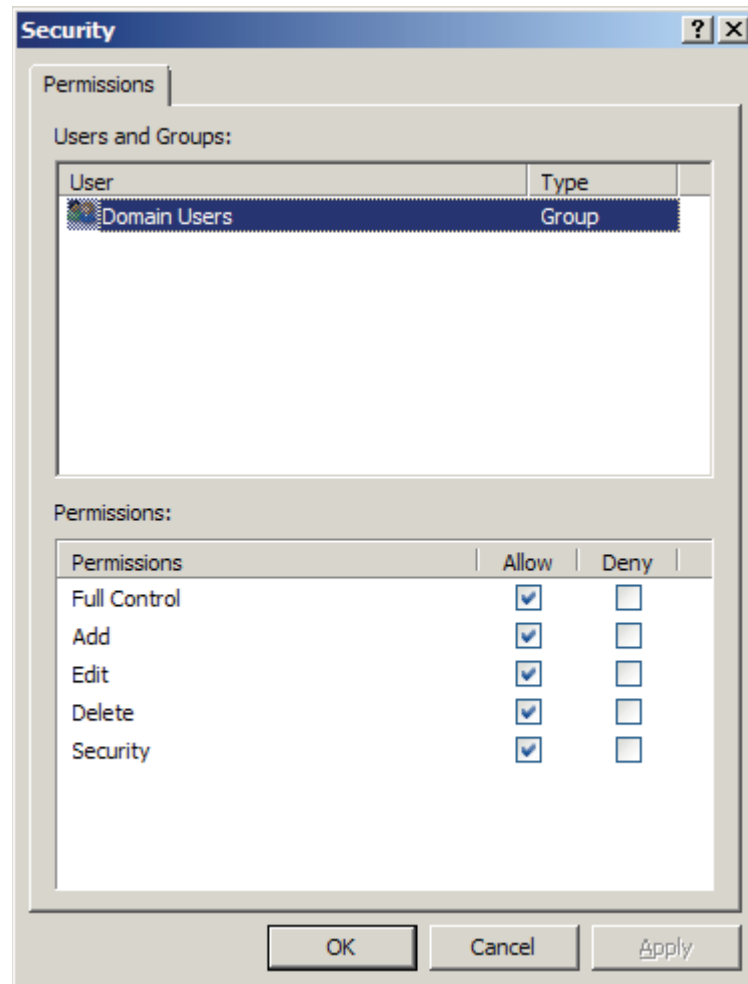
3.3.3 Managing Administrators Access to EMC Nodes

To set the permissions for the specific functionality (for instance, limit Datacenters adding):

1. Select the appropriate tree node, right-click and select **Security**.



2. In the Security window, select the added user/group and select operations you want to allow or deny for them. Then click OK.



3. Permissions for added administrator are defined.

3.4 Managing of Installation Manager

This feature will be added in future versions of Enterprise Management Console

3.5 Managing Isolation Environment

This feature will be added in future versions of Enterprise Management Console

3.5.1 Adding New Isolation Environment

3.5.1.1 Adding Application in Isolation Environment

3.5.1.2 Removing Application in Isolation Environment

3.5.1.3 Managing Rules

3.5.1.4 Specifying Security Options for File Execution

3.5.1.5 Adding New Folder

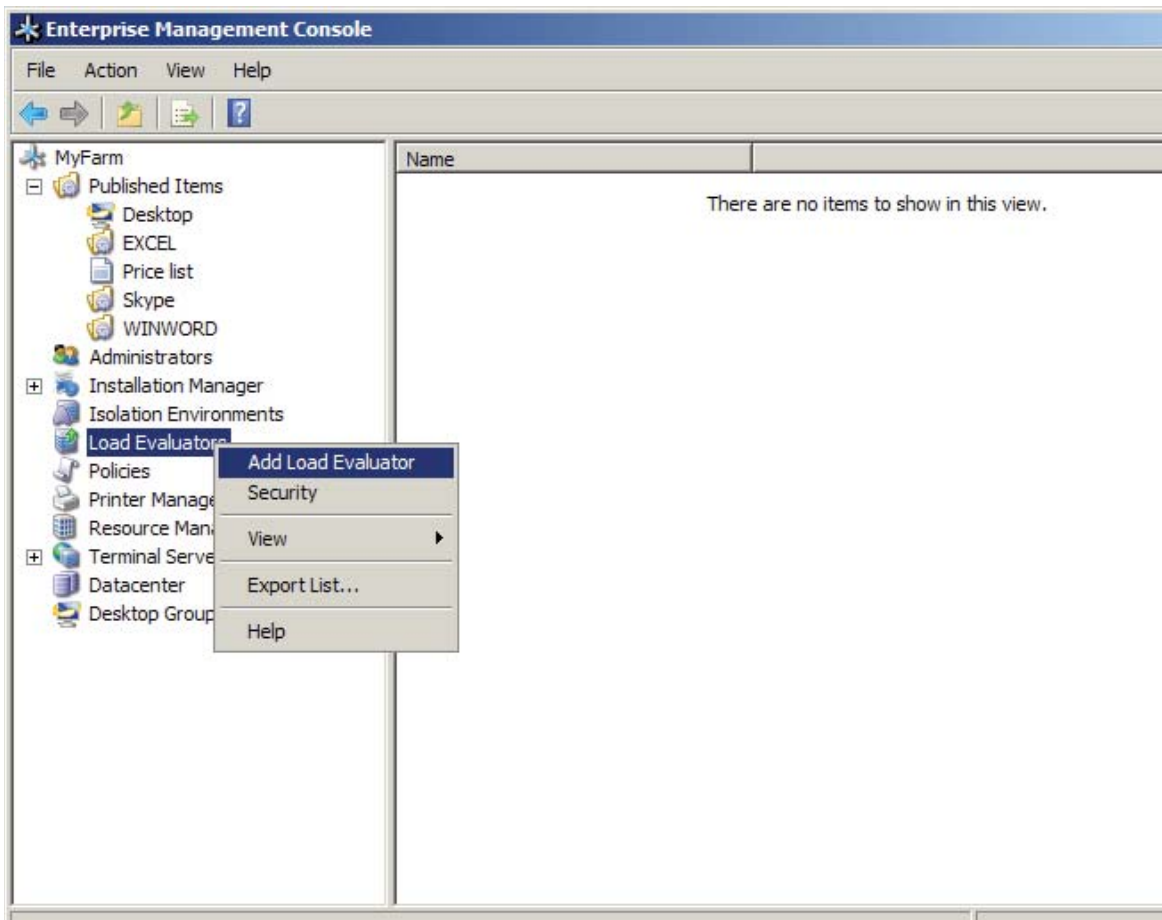
3.6 Smart Load-Balancing

Thinomenon provides smart load-balancing functionality using a concept of Load Evaluators. An appropriate node of Management Console lets administrators to configure parameters for smart load balancing. This feature can be used for Terminal Servers only.

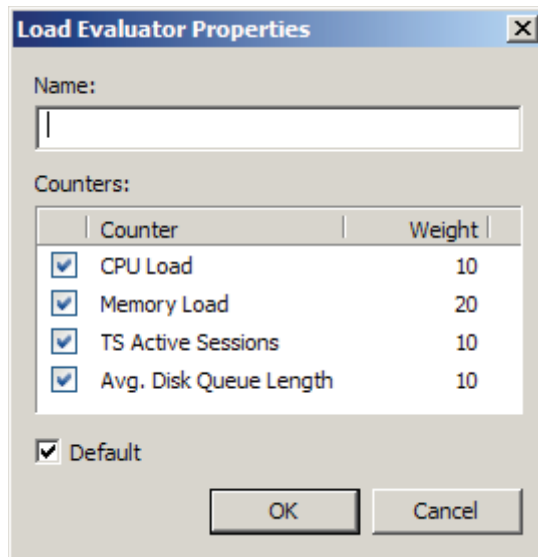
3.6.1 Add Load Evaluator

To add load evaluator:

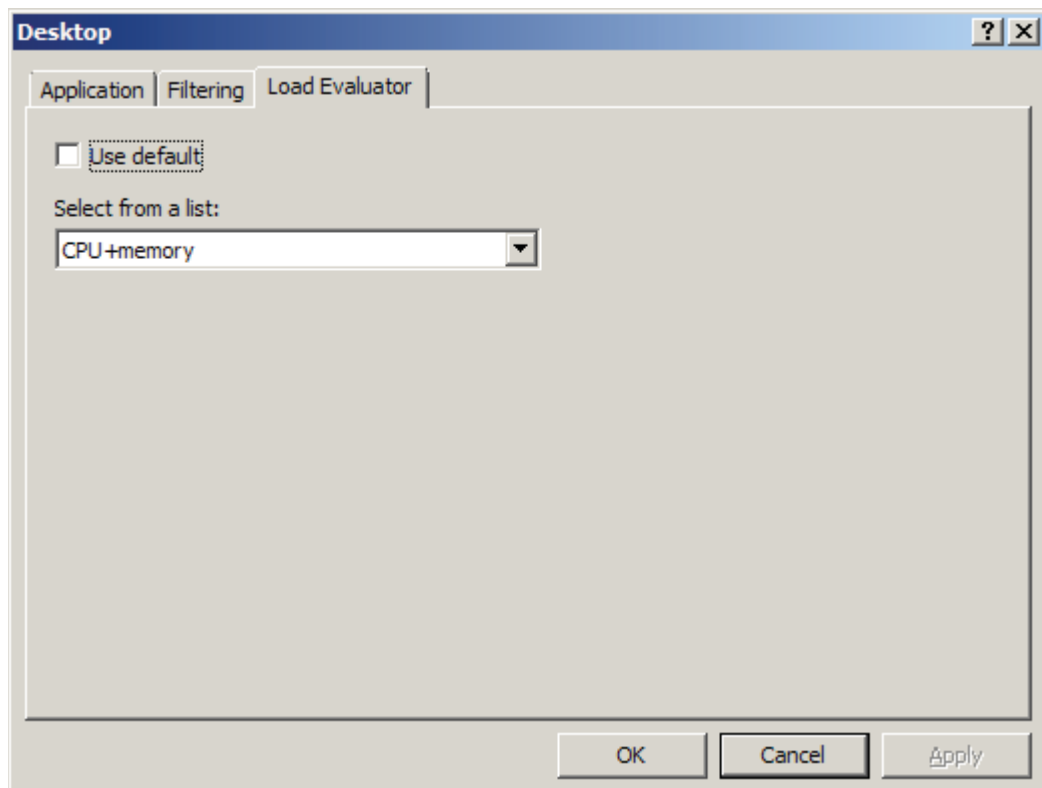
1. Right-click the *Load Evaluators* node and select *Add Load Evaluator*:



2. The *Load Evaluator properties* window opens.



3. Define the Load Evaluator name and check the *Default* option if you want to use this evaluator by default.
4. Select one or more counters and set their weights (the higher is the weight the more important is the counter). Click **OK**.
5. After the load evaluator is created, you can apply it to a specific published item in Terminal Servers infrastructure. To assign a load evaluator to a published item, open the published item Properties and go to *Load Evaluator* tab:



3.6.2 Customizing Load Evaluator

To Customize Load Evaluator:

1. Right-click the Created ***Load Evaluator*** and select ***Properties***
2. Load Evaluator Properties window opens

3.6.3 Delete Load Evaluator

To Delete Load Evaluator:

1. Right-click the Created ***Load Evaluator*** and select ***Delete***
2. Confirmation window appears
3. Click Yes button if you want to delete Load Evaluator, or click No button if not.

3.7 Managing Policies

This feature will be added in future versions of Enterprise Management Console

3.8 Managing Printers

This feature will be added in future versions of Enterprise Management Console.

3.8.1 Setting a Default Printer

3.8.2 Clearing a Default Printer

3.8.3 Removing a Printer

3.8.4 Enabling Client Printing after Setup

3.8.5 Adding Published Printers

3.9 Managing Resource Manager

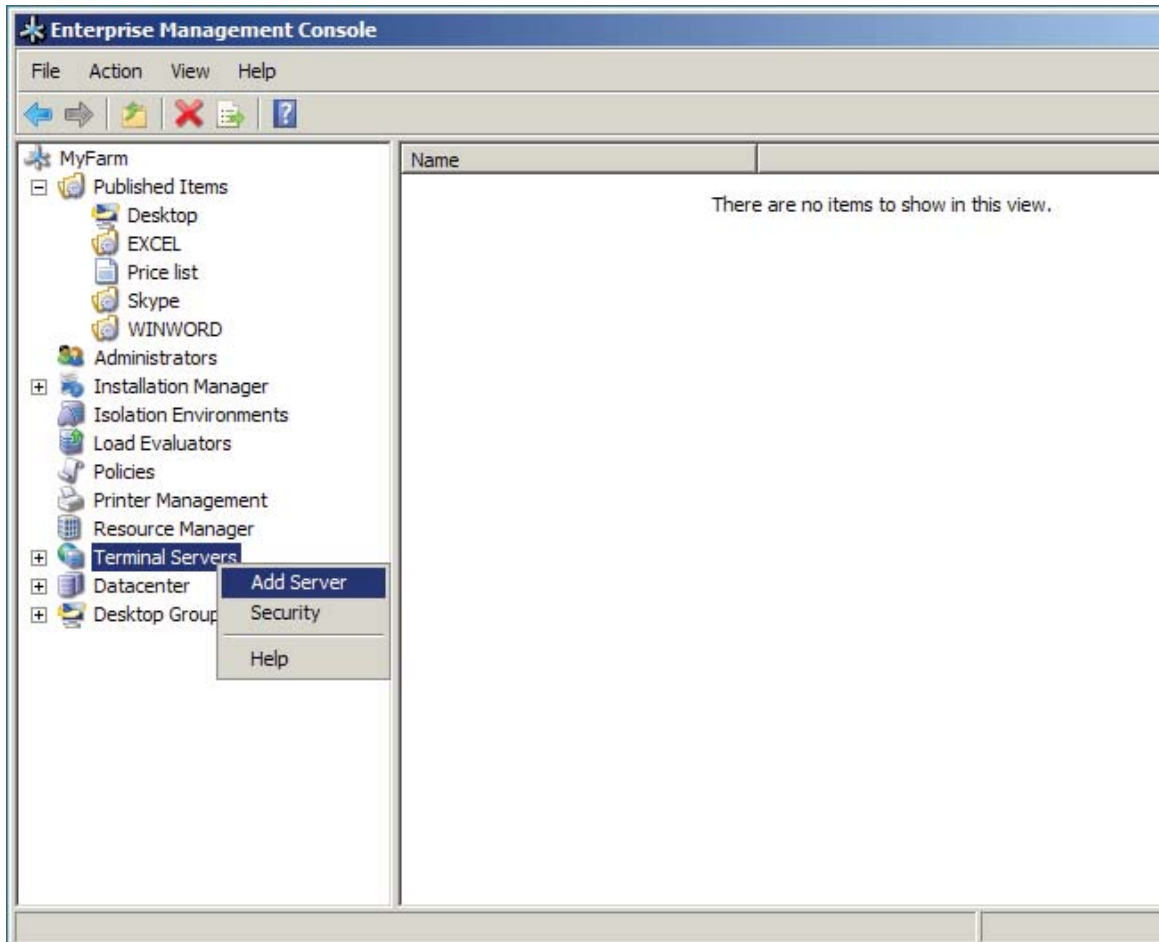
This feature will be added in future versions of Enterprise Management Console.

3.10 Managing Terminal Servers

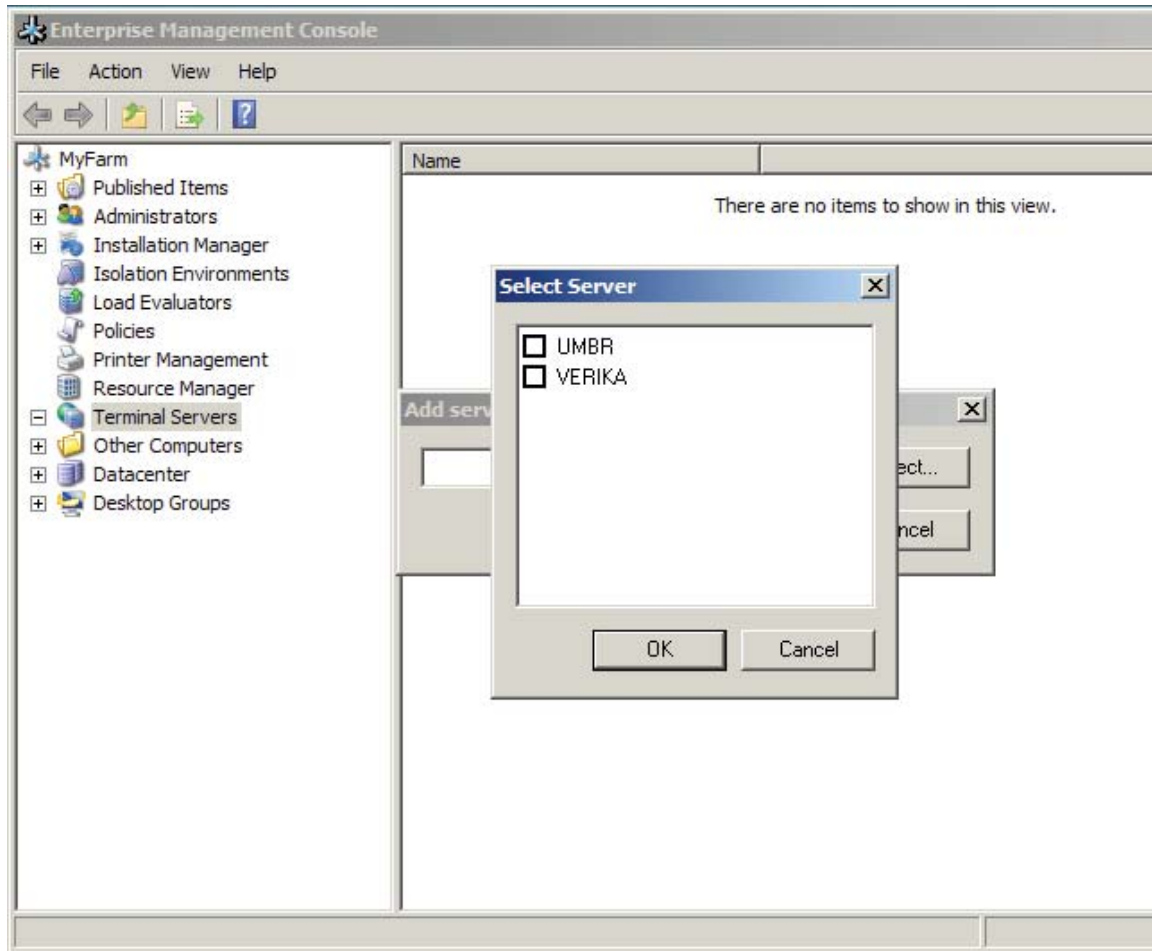
3.10.1 Add Terminal Server

To add Terminal Server to Enterprise Management Console:

1. Right-click the **Terminal Servers** node and select **Add Server** :



2. Click **Select** to browse all compatible hosts from the local subnet and select the necessary hosts. Click **OK**



3.10.2 Connect to Added Terminal Server

To connect to Added Terminal Server:

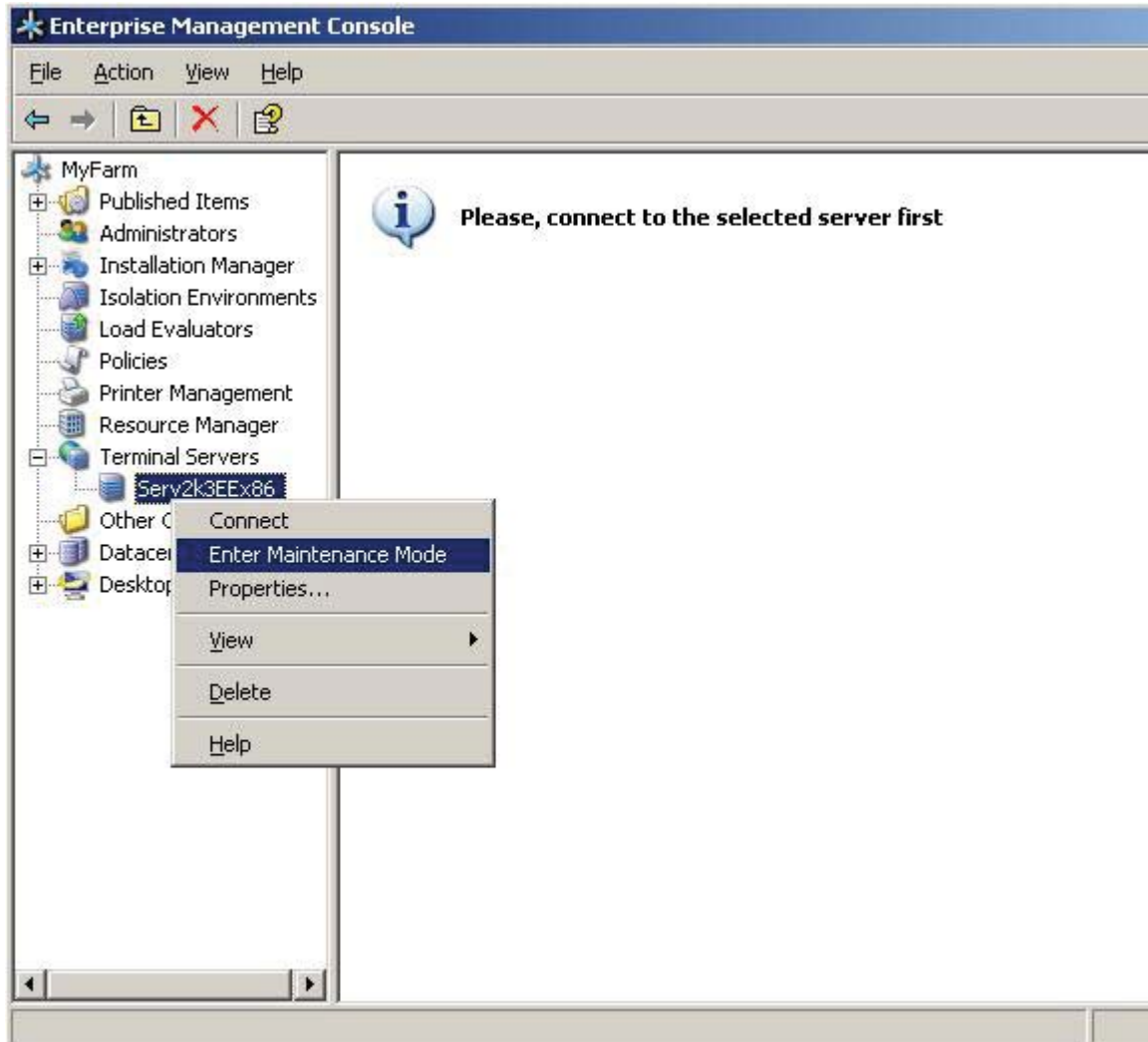
1. Right-click the *Added Terminal Servers* node and select **Connect**

3.10.3 Performing Server Maintenance

3.10.3.1 To perform server maintenance

To Enter maintenance mode:

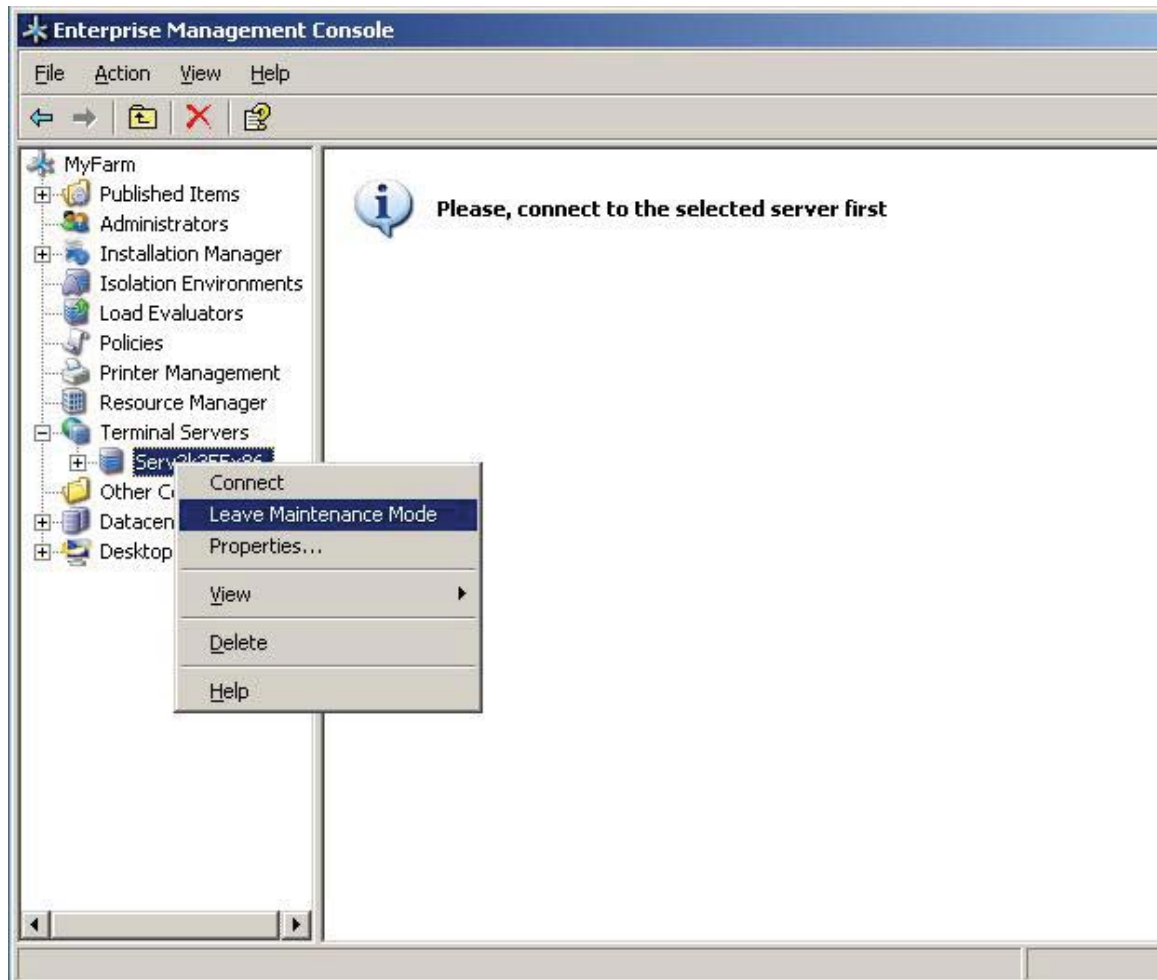
1. Right click the server and select Enter Maintenance Mode.



3.10.3.2 To restore a server after maintenance

To exit maintenance mode:

1. Right click the server and select Leave Maintenance Mode.

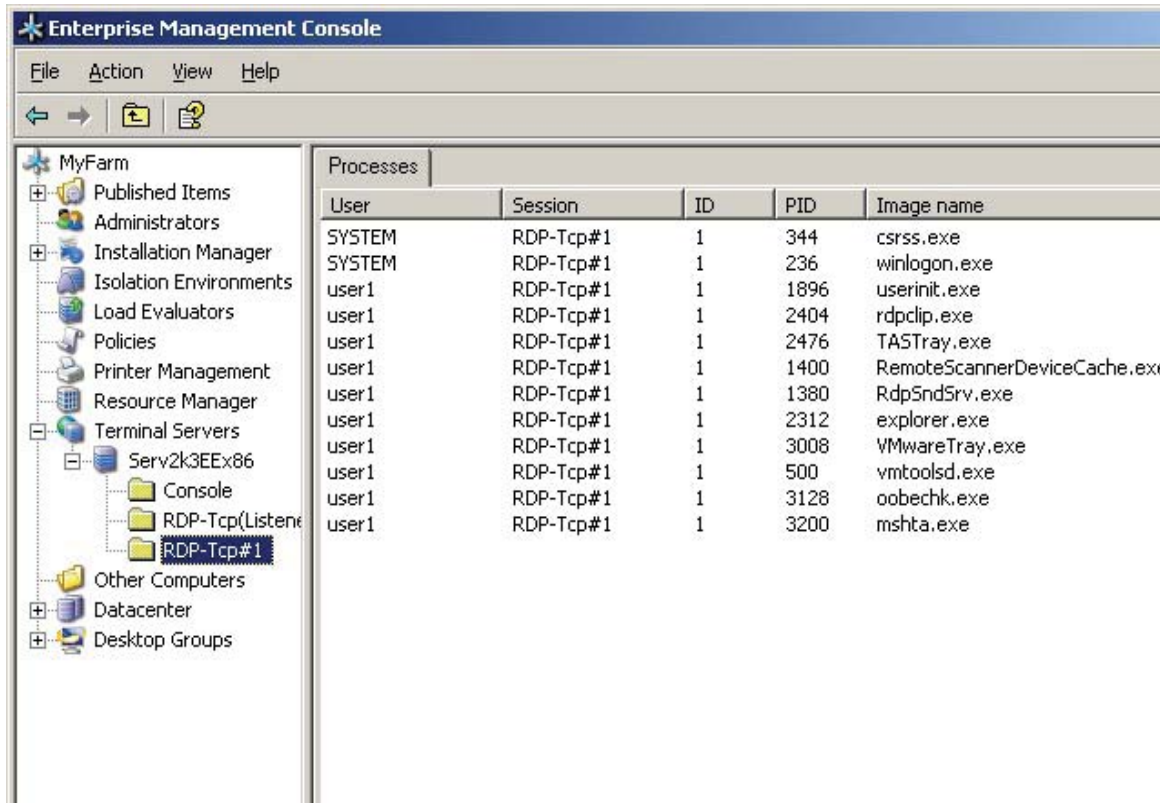


3.10.4 Managing Sessions

3.10.4.1 Viewing Session Details

To view Session Details:

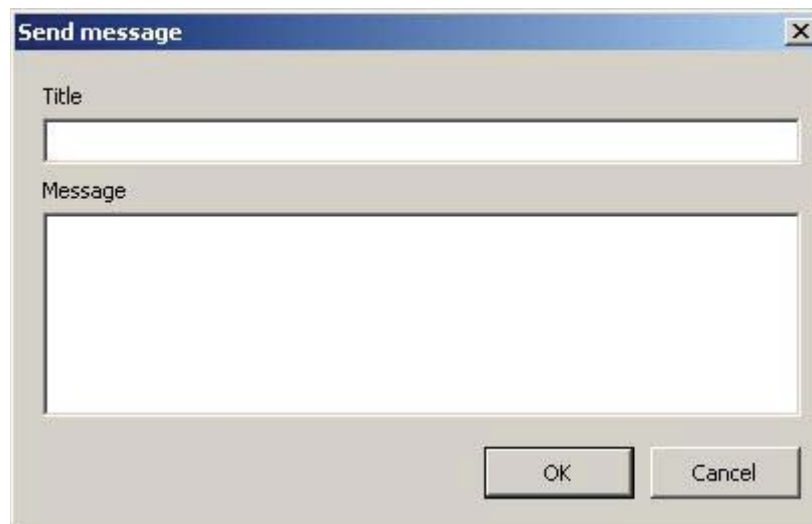
1. Connect to added Terminal Server
2. Click on active session that you want to view.



3.10.4.2 Sending Messages

To Send Messages:

1. Connect to Added Terminal Server
2. Right click Session or User you want to send message and select Send Message. The *Send Message* dialog box appears



3. Enter the content of the message
4. Click **OK**. The message is sent immediately to the selected user or session.

3.10.4.3 Ending Sessions

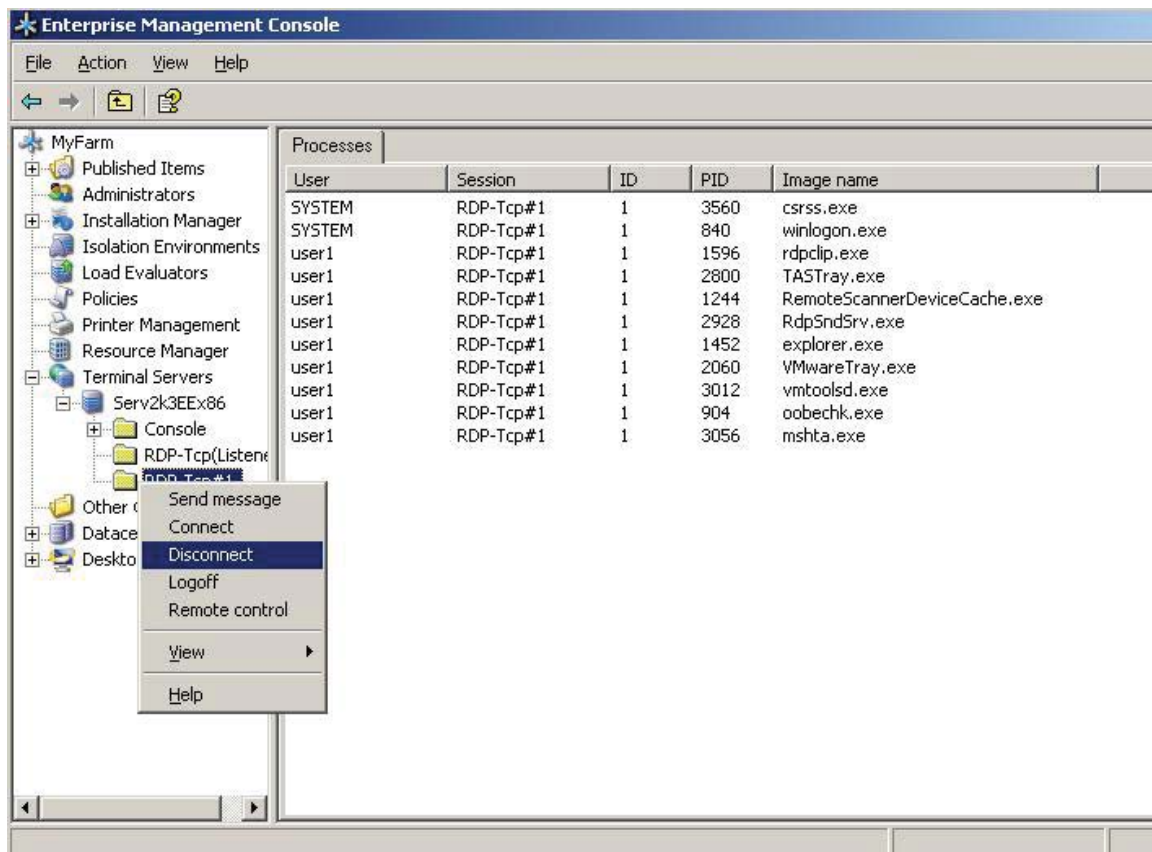
To End sessions:

1. Connect to Added Terminal Server
2. Right click User you want to Logoff select Log off. **Confirmation Window** appears.
3. Click **Yes** if you are sure you want to Logoff this session.

3.10.4.4 Disconnecting Sessions

To Disconnect sessions:

1. Connect to Added Terminal Server
2. Right click Session you want to Disconnect select Disconnect. **Confirmation Window** appears.



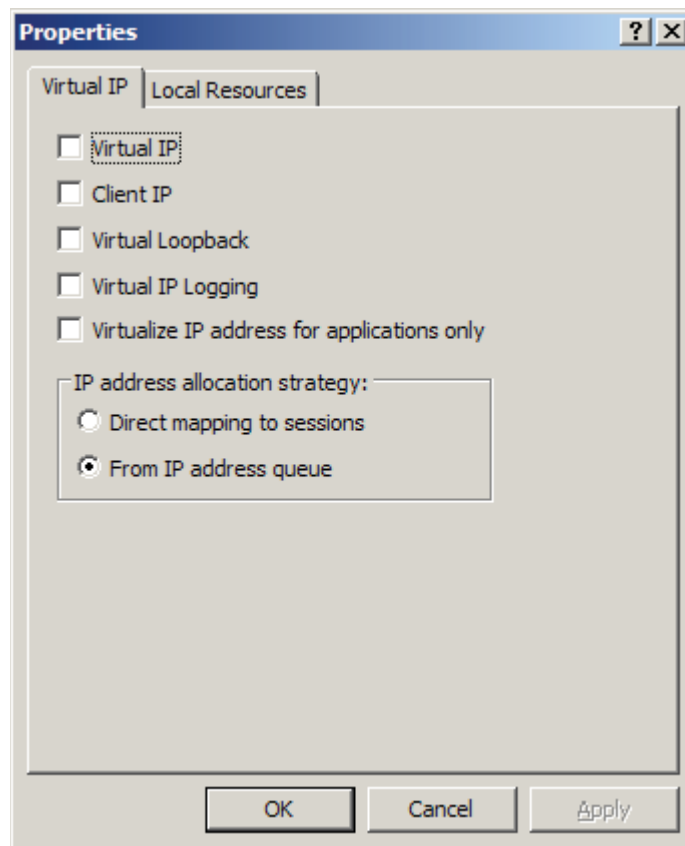
3. Click **Yes** if you are sure you want to Logoff this session.



3.10.5. Virtual IP management

Virtual IP is necessary to make existing applications compatible with some software packages and/or hardware appliances¹ that use IP addresses as means to identity and/or authenticate users/sessions. Virtual IP address option actually assigns multiple IP addresses to the network card and therefore virtualized IP addresses are visible both within the application and on the network.

To turn on IP virtualization, open the Properties of Member Server in EMC and check the appropriate option:



3.10.5.1 Enable Virtual IP feature

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Check Virtual IP option. Click **OK**

3.10.5.2 Enable Using Client IP in Session

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Check Client IP option. Click **OK**

¹ Such as popular filtering firewall appliances manufactured by multiple vendors.

3.10.5.3 Enable Loopback Virtualization

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Check Virtual Loopback option. Click **OK**

3.10.5.4 Enable Virtual IP Logging

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Check Virtual IP Logging option. Click **OK**

3.10.5.5 Enable IP address Virtualization for application only

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Check Virtualize IP address for application option. Click **OK**

3.10.5.6 Change IP Addresses allocation strategy

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Select IP address allocation strategy that you want to use. Click **OK**

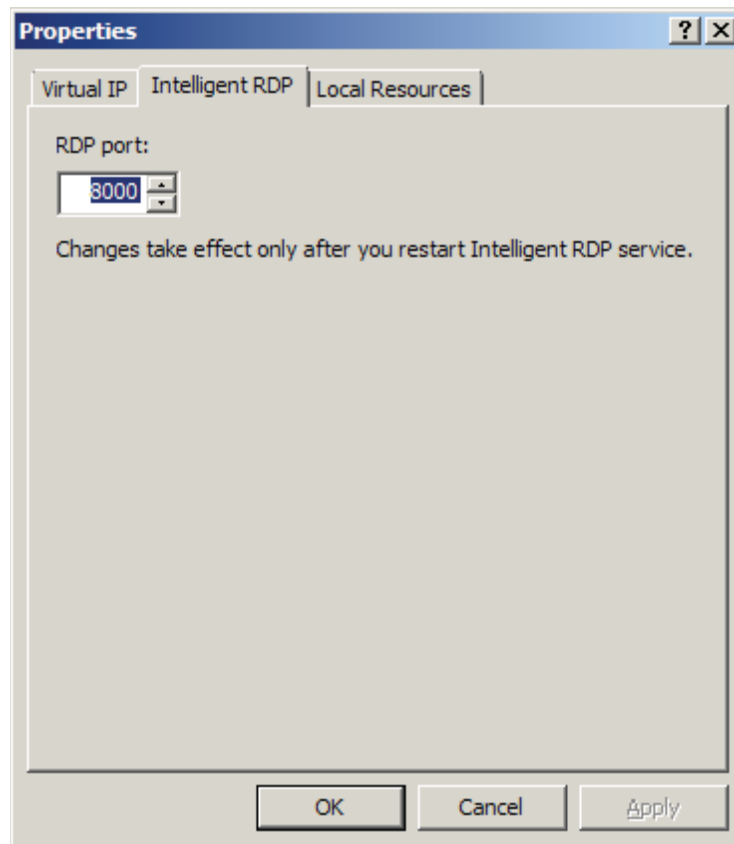
3.10.6 Managing Local Resources

Local Resources tab allows administrator to set a server-wide policy for sharing resources between clients and the server. When resource sharing is enabled at the server-level, administrators can still adjust settings for individual users or groups using Group Policy and other Windows policy configuration tools.

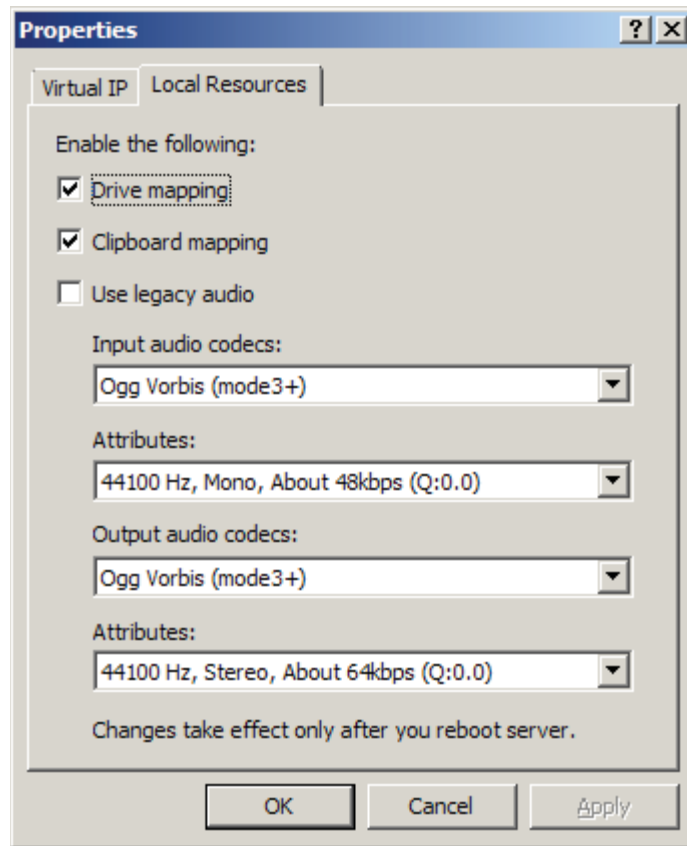
In addition to common options such as disk drive and clipboard redirection, Thinomenon includes advanced multimedia acceleration capabilities.

Member Server running Windows Server 2003 has the additional adjustment tab for Intelligent RDP. Windows Server 2008 and later does not need a separate Intelligent RDP service and/or port. Therefore, this tab will not be displayed as part of server properties configuration.

From **Intelligent RDP** tab you can adjust RDP port for Thinomenon Intelligent RDP service. Typically, the default port will work for most situations.



Local Resource tab:



3.10.6.1 Enable Drive mapping

To enable Drive mapping:

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Go to Local Resources tab.
3. Check Drive mapping option. Click **OK**

3.10.6.2 Enable Clipboard mapping

To enable Clipboard mapping

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Go to Local Resources tab.
3. Check Clipboard mapping option. Click **OK**

3.10.6.3 Enable using legacy audio

To enable usage of legacy audio:

1. Select **Properties** item from right-click menu of specific Terminal Server.
2. Go to Local Resources tab.
3. Check Use legacy audio option. Click **OK**

3.10.6.4 Modify audio settings

Thinomenon Access Suite includes a virtual audio driver virtualizing Windows audio support and making multimedia applications compatible with running in remote sessions.

1. Select Properties item from right-click menu of specific Terminal Server.
2. Go to Local Resources tab.
3. Modify audio settings. Click OK

3.11 Managing Other Computers node

3.11.1 Adding Computers to Other Computers node

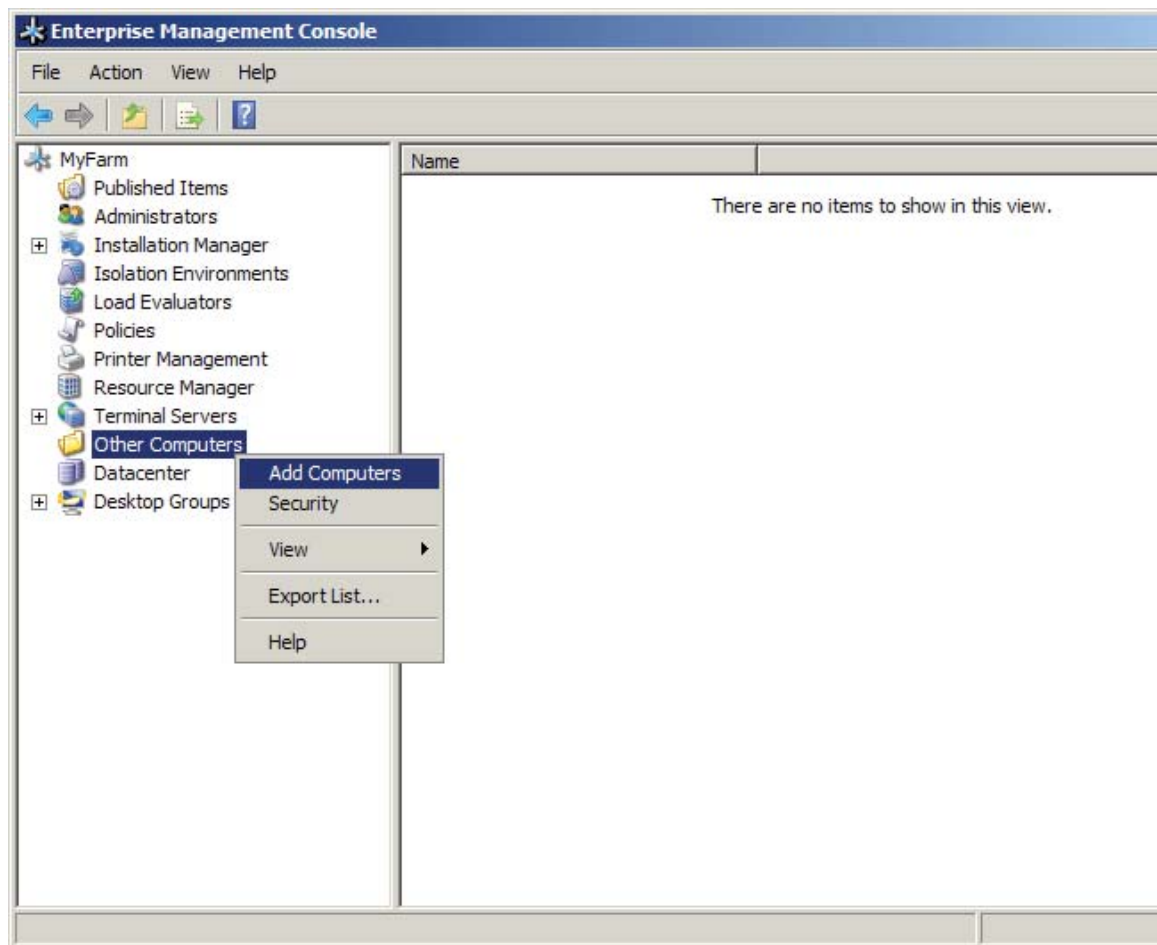
3.11.1.1 Add computer by Browsing Network/Active Directory

This functionality will be created in future

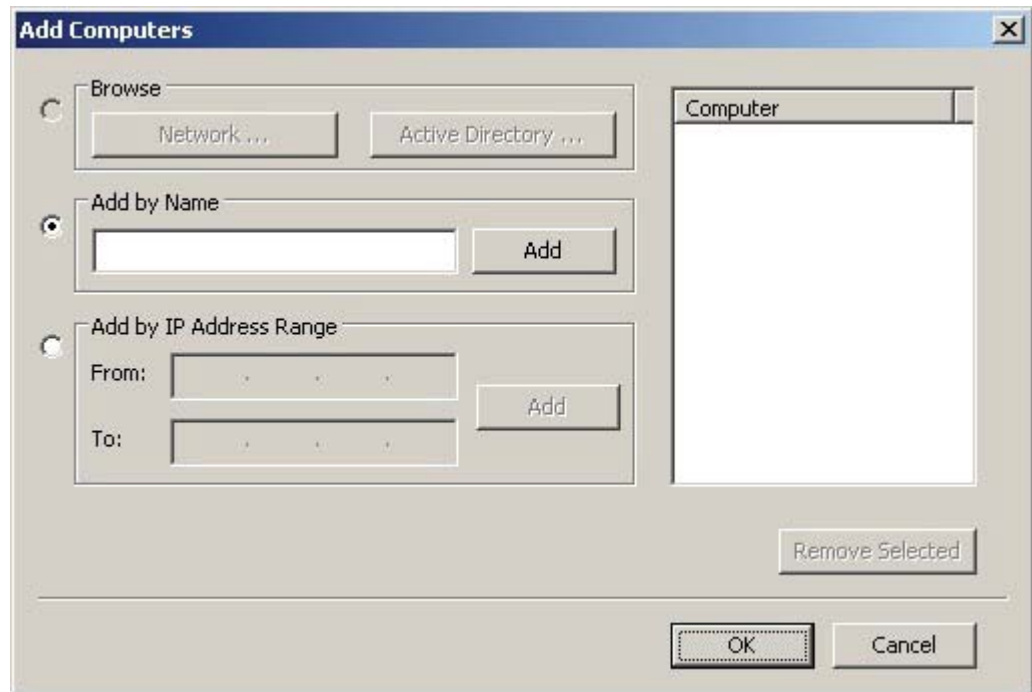
3.11.1.2 Add computer by Name/IP

To add physical computer to EMC by Name/IP:

1. Right-click **Other Computers** node and select **Add Computers** item:



Add Computers dialog appears:



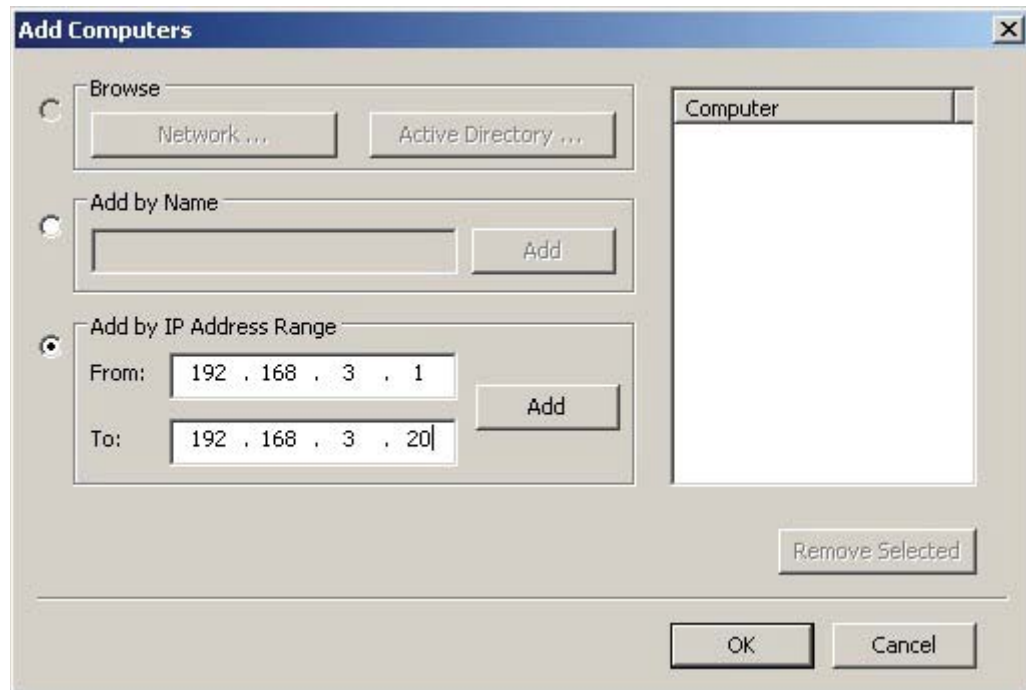
2. In Add by Name field specify Computer name or its IP and then click Add;
3. Click **OK**

3.11.1.3 Add computer by IP Address Range

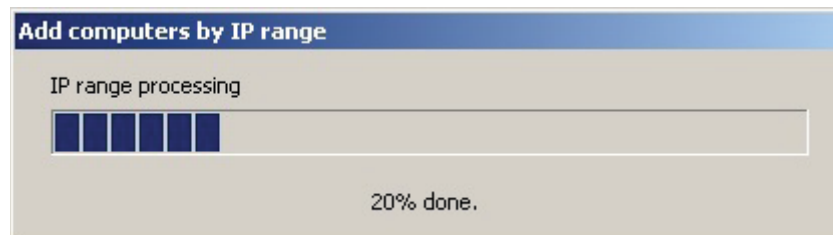
To add physical computer to EMC by IP Address Range:

1. Right-click **Other Computers** node and select *Add Computers* item.

Add Computers dialog appears



2. Select Add by IP Address Range radio-button
3. Specify IP range. Click *Add*
4. Add computers by IP range process starts



5. Click *OK*

3.12 Working with Datacenters

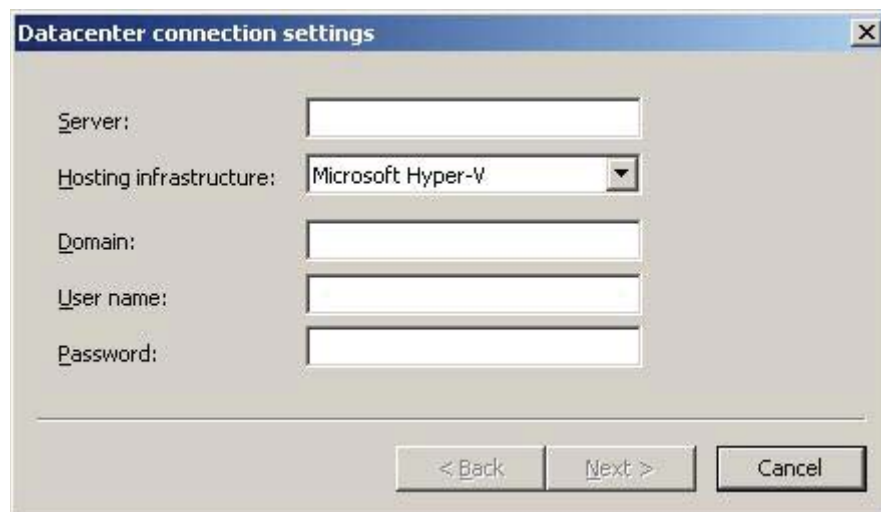
Requirements:

1. There must be virtual machine(s) or template(s) on VDI provider.

3.12.1 Add Datacenter to EMC

To add Datacenter to Management Console:

1. Select **Add Asset** item from right-click menu of **Datacenter** node. Datacenter connection settings window appears.



The screenshot shows a dialog box titled "Datacenter connection settings". It has five input fields: "Server:", "Hosting infrastructure:" (with a dropdown menu showing "Microsoft Hyper-V"), "Domain:", "User name:", and "Password:". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

2. Specify Connection settings. Click **Next**
3. Select a template(s) among displayed virtual machines to create new machines from this template. Click **Finish** to complete wizard

3.12.2 Delete Datacenter from EMC

To Delete Datacenter from EMC:

1. Select **Delete** item from Created Datacenter right-click menu. **Confirmation window** appears.



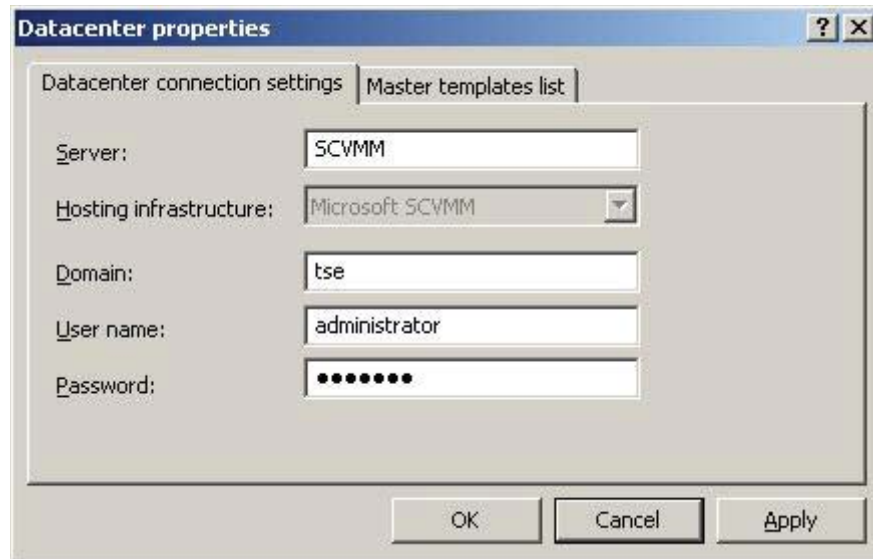
The screenshot shows a dialog box titled "Confirmation". It contains a question mark icon and the text: "Are you sure you want to delete this server?" and "All desktop groups that belong to this server will be deleted as well." At the bottom, there are two buttons: "Yes" and "No".

2. Click **Yes** if you sure to delete this Datacenter.

3.12.3 Modify Connection Properties of added Datacenters

To modify connection properties of added Datacenter:

1. Select **Properties** item from Created Datacenter right-click menu.

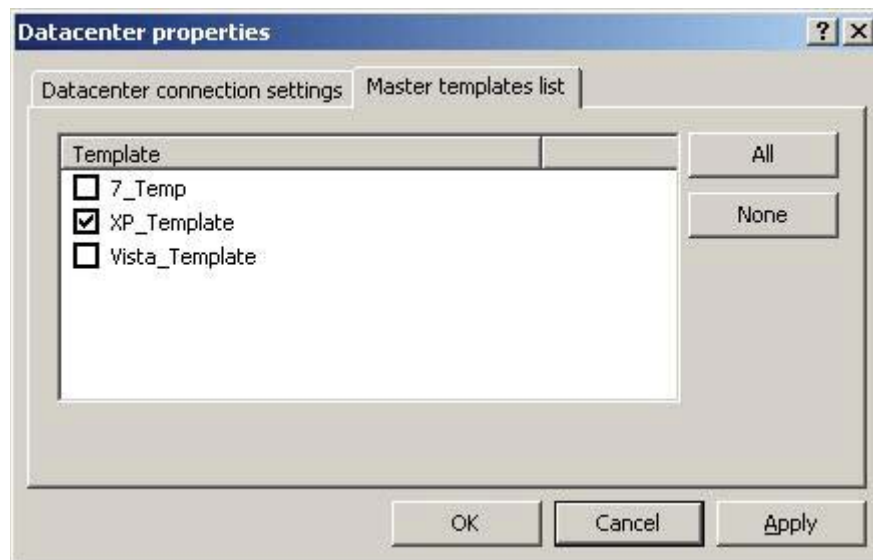


2. Change Datacenter connection settings. Click **OK**

3.12.4 Add/Delete Templates in Master Template list

To Add or Delete templates in Master Template list:

1. Select **Properties** item from Created Datacenter right-click menu.
2. Go to Master templates list tab



3. Select templates you want to add or delete. Click **OK**

3.12.5 Refresh list of VMs in Datacenter

To Refresh List of VMs in Datacenter:

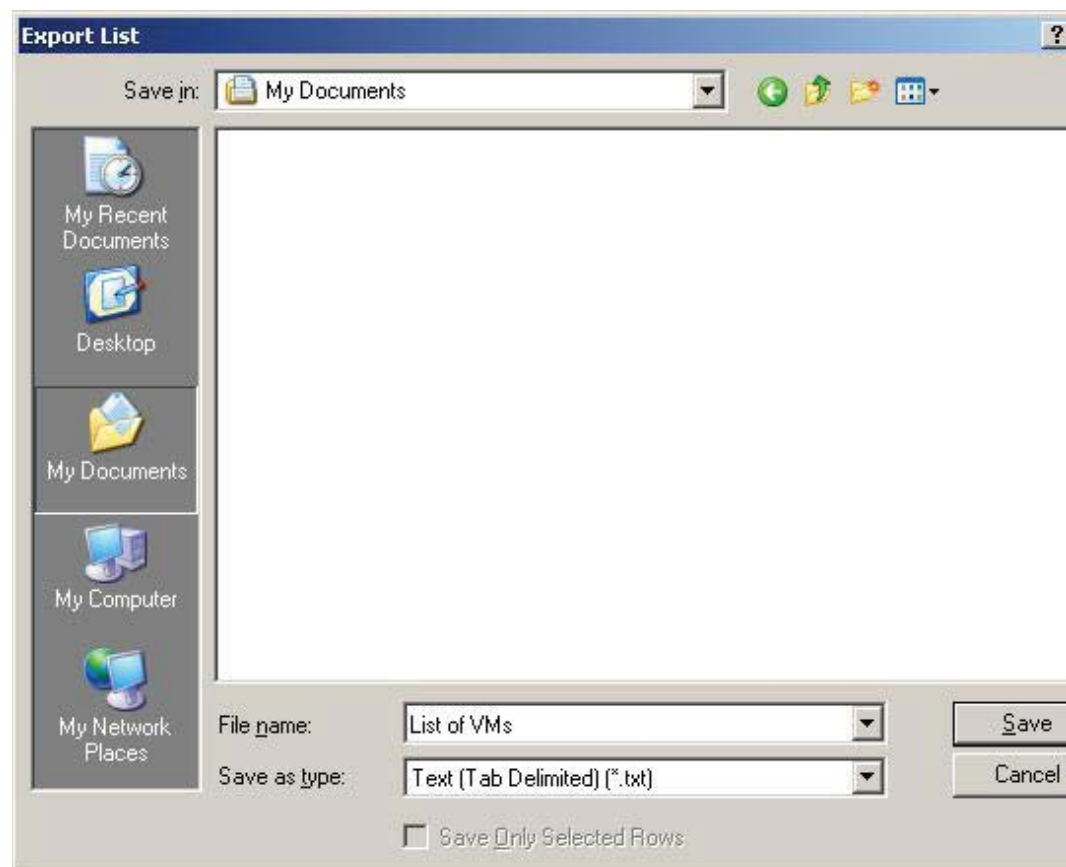
1. Select **Refresh** item from Created Datacenter right-click menu.



3.12.6 Export list of VMs

To Export list of VMs:

1. Select **Export List** item from Created Datacenter right-click menu.
2. Specify Path and File name for List. Click **Save**

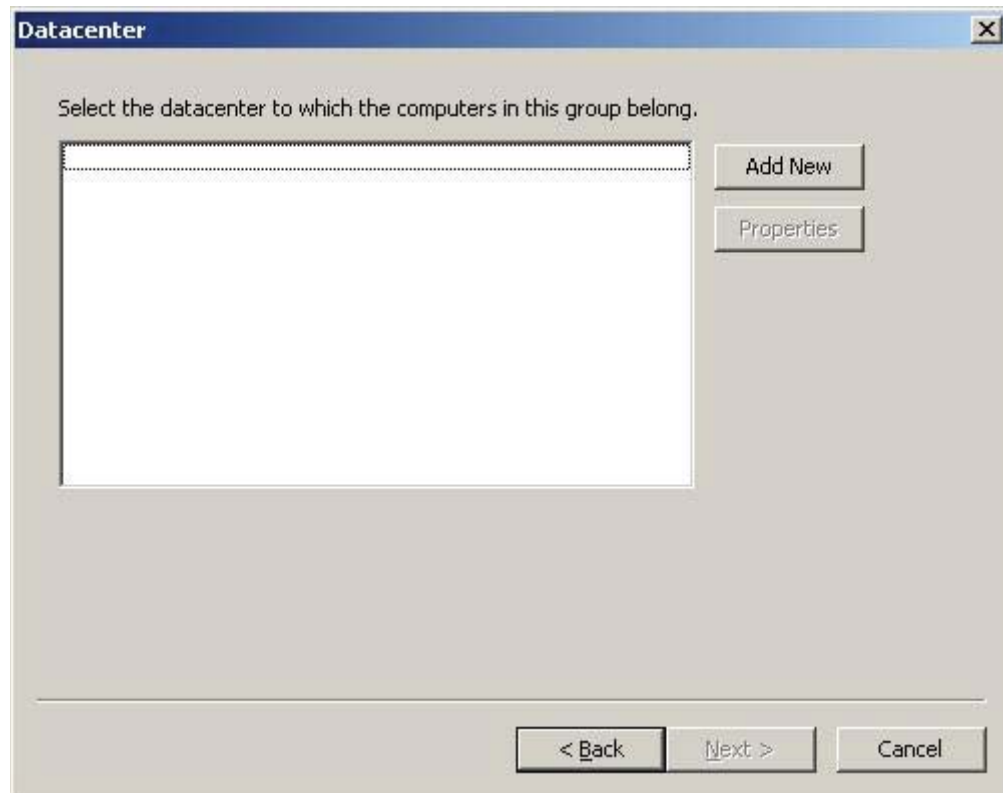


3.12.7 Add Datacenter from Desktop Group creation wizard

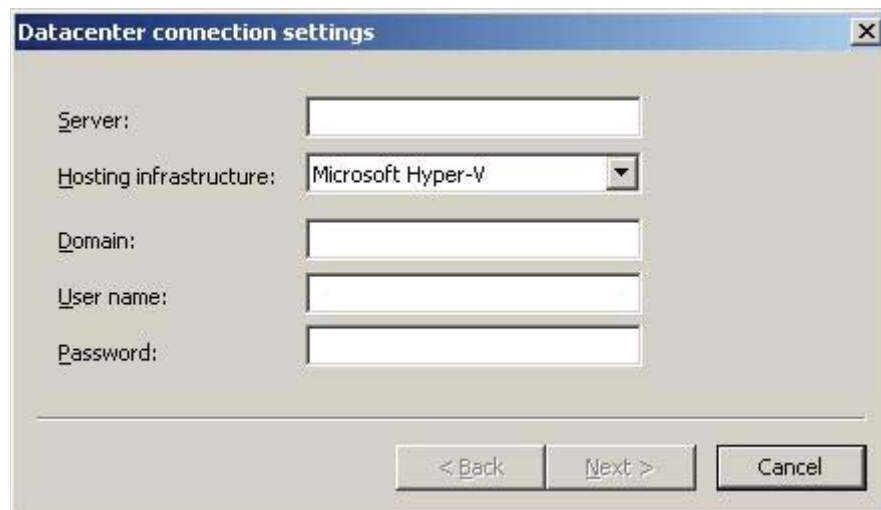
To **add** Datacenter from Desktop Group creation wizard:

1. Select **New Group** item from Desktop Groups right-click menu. Click **Next**
2. Enter friendly name for Desktop Group. Click **Next**
3. Select VDI hosting infrastructure for this group. Click **Next**. **Datacenter Win-**

dow appears.



4. Click **Add New** button. Datacenter connection settings window appears.



5. Specify Connection settings. Click **Next**

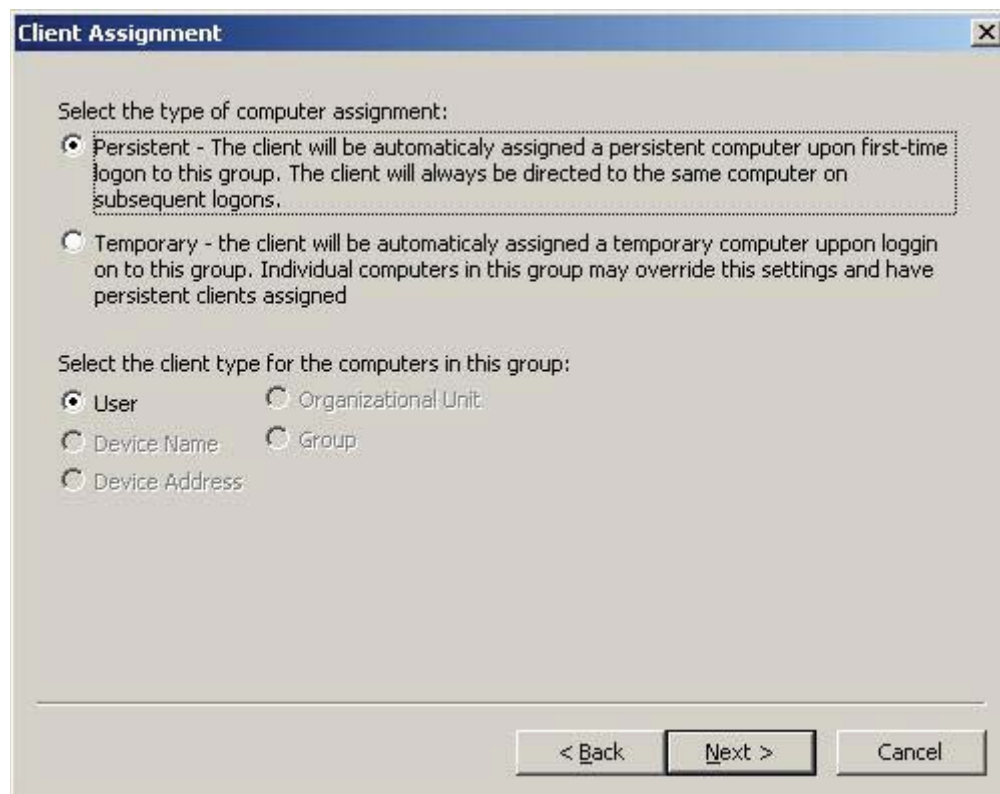
6. Select a template(s) among displayed virtual machines to create new machines from this template. Click **Finish** to complete wizard

3.13 Creating and Updating Desktop Groups

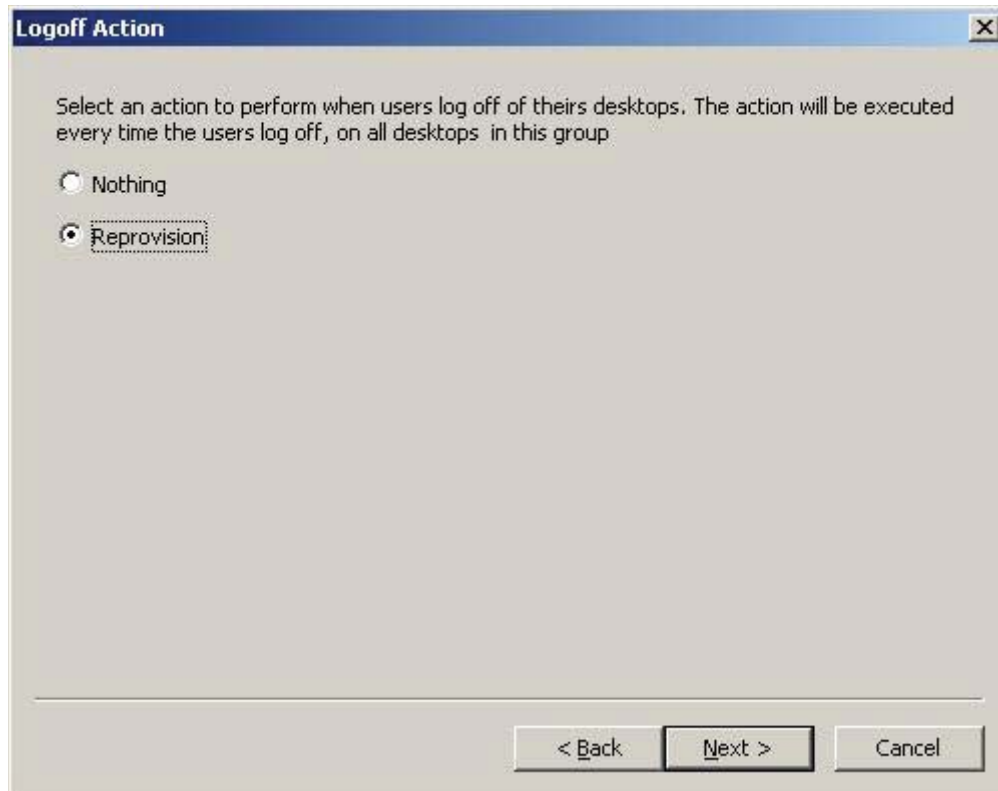
3.13.1 Create Persistent Desktop Group with Reprovision Logoff action for VDI

To create Persistent Desktop Group with Reprovision Logoff action for VDI:

1. Select **New Group** item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click **Next**
3. Select VDI hosting infrastructure for this group. Click **Next**
4. Select Datacenter from the list. Click **Next**
5. Specify Password for local Administrator. Click **Next**
6. Select **Persistent** type of Client Assignment. Click **Next**

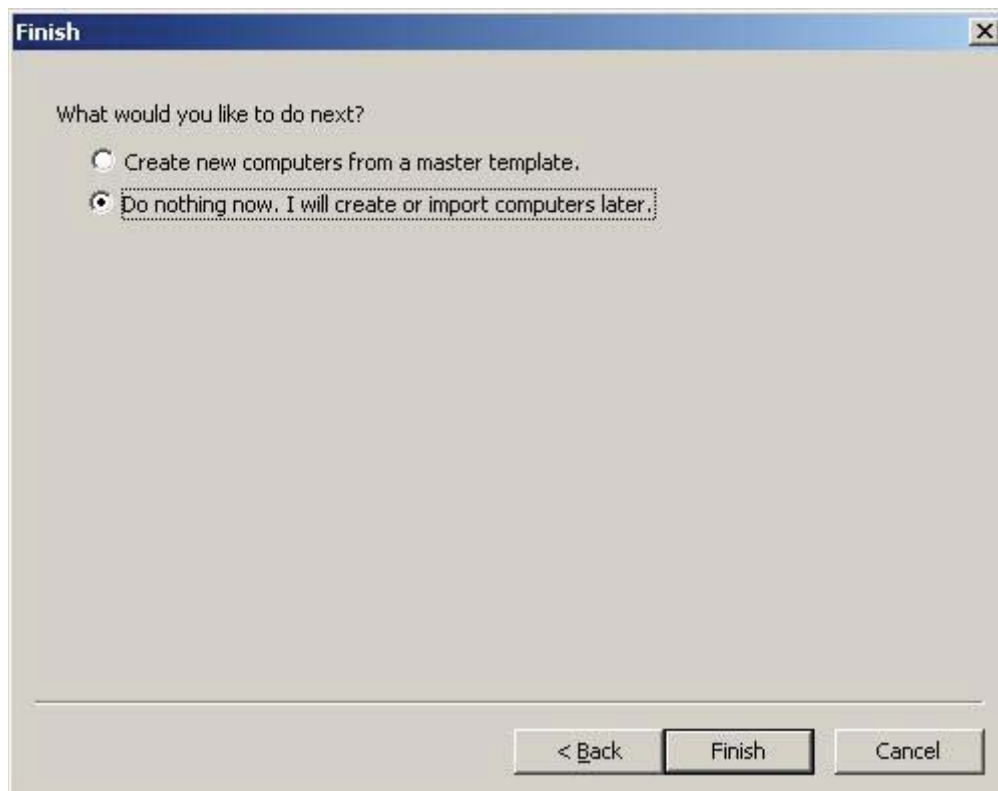


7. Choose User Privileges. Click **Next**
8. Select process for Session Auto-Logoff or add new one. Click **Next**
9. Select **Reprovision** Logoff action. Click **Next**



10. Enable/Disable Auto-Expand. Click *Next*

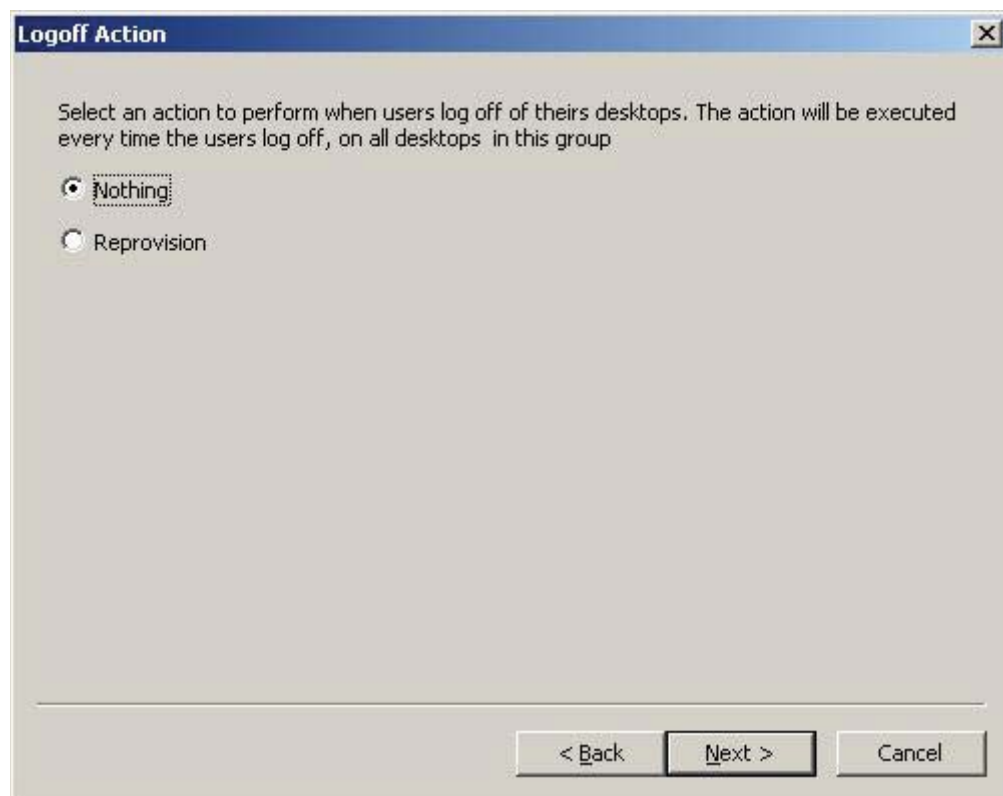
11. Select Do nothing, I will create or import computers later. Click *Finish* to complete the wizard



3.13.2 Create Persistent Desktop Group with No Logoff action for VDI

To create Persistent Desktop Group with No Logoff action for VDI:

1. Select **New Group** item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click **Next**
3. Select VDI hosting infrastructure for this group. Click **Next**
4. Select Datacenter from the list. Click **Next**
5. Specify Password for local Administrator. Click **Next**
6. Select **Persistent** type of Client Assignment. Click **Next**
7. Choose User Privileges. Click **Next**
8. Select process for Session Auto-Logoff or add new one. Click **Next**
9. Select **Nothing** Logoff action. Click **Next**



10. Enable/Disable Auto-Expand. Click **Next**
11. Select Do nothing. I will create or import computers later. Click **Finish** to complete the wizard

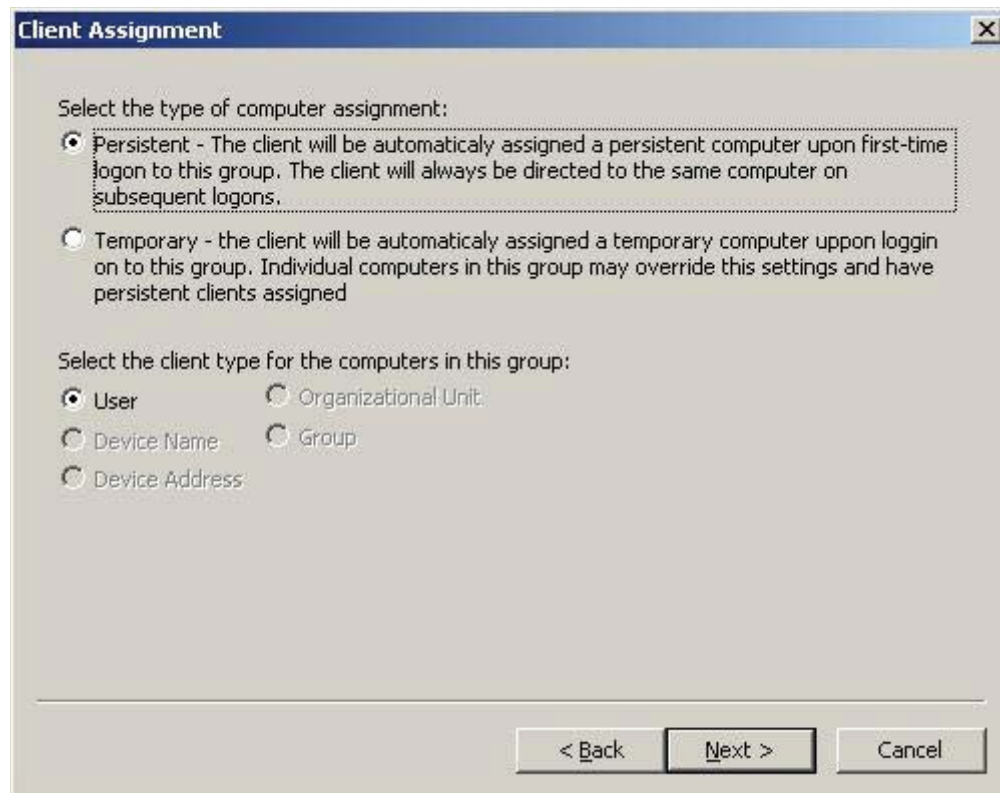
3.13.3 Create Persistent Desktop Group for Other/Physical

To create Persistent Desktop Group for Other/Physical:

1. Select **New Group** item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click **Next**
3. Select **Other/Physical** hosting infrastructure for this group. Click **Next**



4. Specify Password for local Administrator. Click **Next**
5. Select **Persistent** type of Client Assignment. Click **Next**

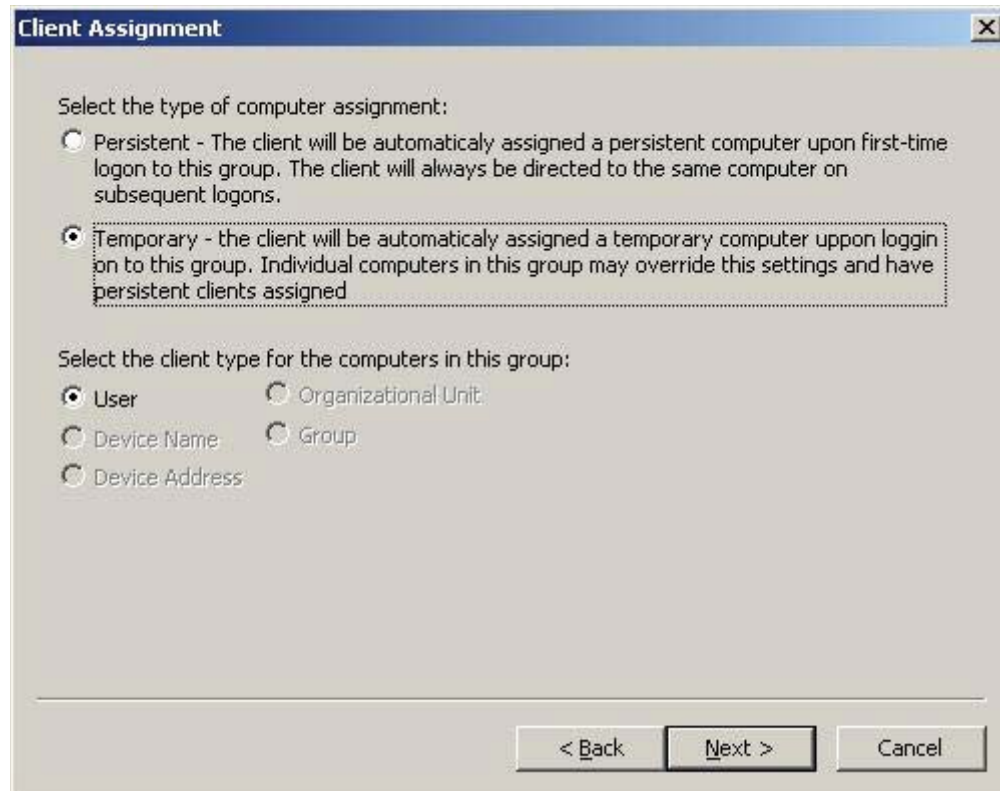


6. Choose User Privileges. Click **Next**
7. Select process for Session Auto-Logoff or add new one. Click **Next**
8. Select Do nothing. I will add computers later. Click **Finish** to complete the wizard

3.13.4 Create Temporary Desktop Group with Reprovision Logoff action for VDI

To create Temporary Desktop Group with Reprovision Logoff action for VDI:

1. Select **New Group** item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click **Next**
3. Select VDI hosting infrastructure for this group. Click **Next**
4. Select Datacenter from the list. Click **Next**
5. Specify Password for local Administrator. Click **Next**
6. Select **Temporary** type of Client Assignment. Click **Next**



The 'Client Assignment' dialog box has a title bar with a close button. It contains two sections. The first section, 'Select the type of computer assignment:', has two radio buttons: 'Persistent' (unselected) and 'Temporary' (selected). The 'Temporary' option is enclosed in a dashed border. The second section, 'Select the client type for the computers in this group:', has four radio buttons: 'User' (selected), 'Organizational Unit' (unselected), 'Device Name' (unselected), and 'Device Address' (unselected). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Select the type of computer assignment:

- ☐ Persistent - The client will be automatically assigned a persistent computer upon first-time logon to this group. The client will always be directed to the same computer on subsequent logons.
- ☒ Temporary - the client will be automatically assigned a temporary computer upon logging on to this group. Individual computers in this group may override this settings and have persistent clients assigned

Select the client type for the computers in this group:

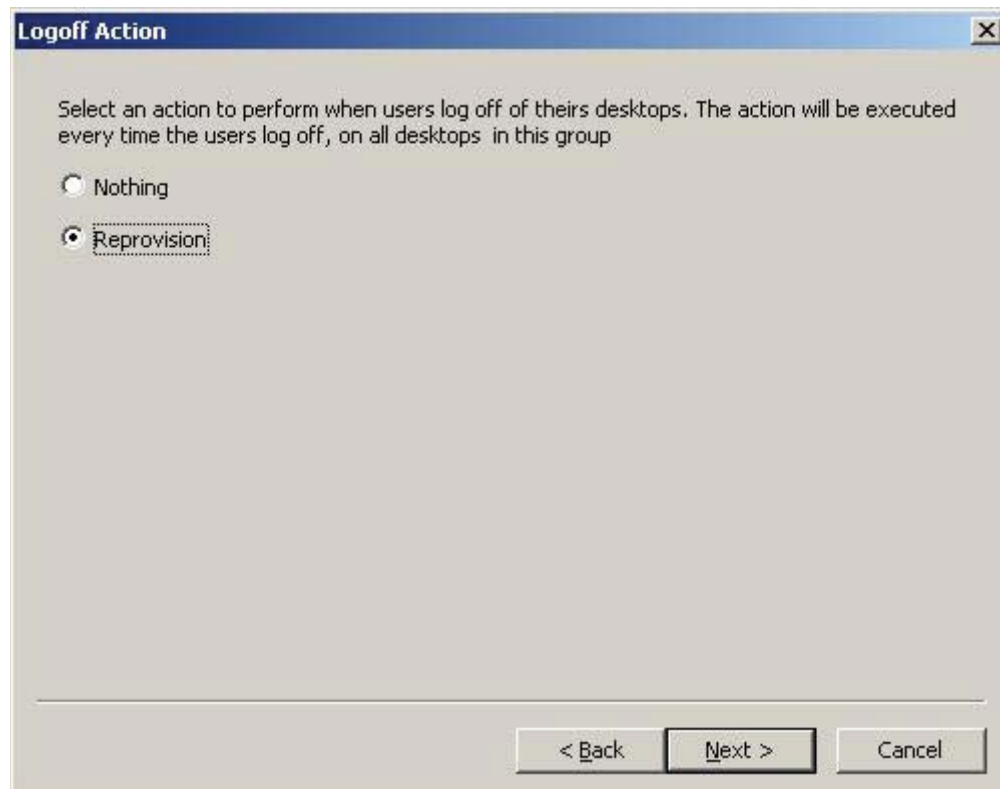
- ☒ User
- ☐ Organizational Unit
- ☐ Device Name
- ☐ Device Address
- ☐ Group

< Back Next > Cancel

7. Choose User Privileges. Click *Next*

8. Select process for Session Auto-Logoff or add new one. Click *Next*

9. Select **Reprovision** Logoff action. Click *Next*



The 'Logoff Action' dialog box has a title bar with a close button. It contains a text instruction and two radio buttons. The text says: 'Select an action to perform when users log off of their desktops. The action will be executed every time the users log off, on all desktops in this group.' The two radio buttons are 'Nothing' (unselected) and 'Reprovision' (selected). The 'Reprovision' option is enclosed in a dashed border. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Select an action to perform when users log off of their desktops. The action will be executed every time the users log off, on all desktops in this group.

- ☐ Nothing
- ☒ Reprovision

< Back Next > Cancel

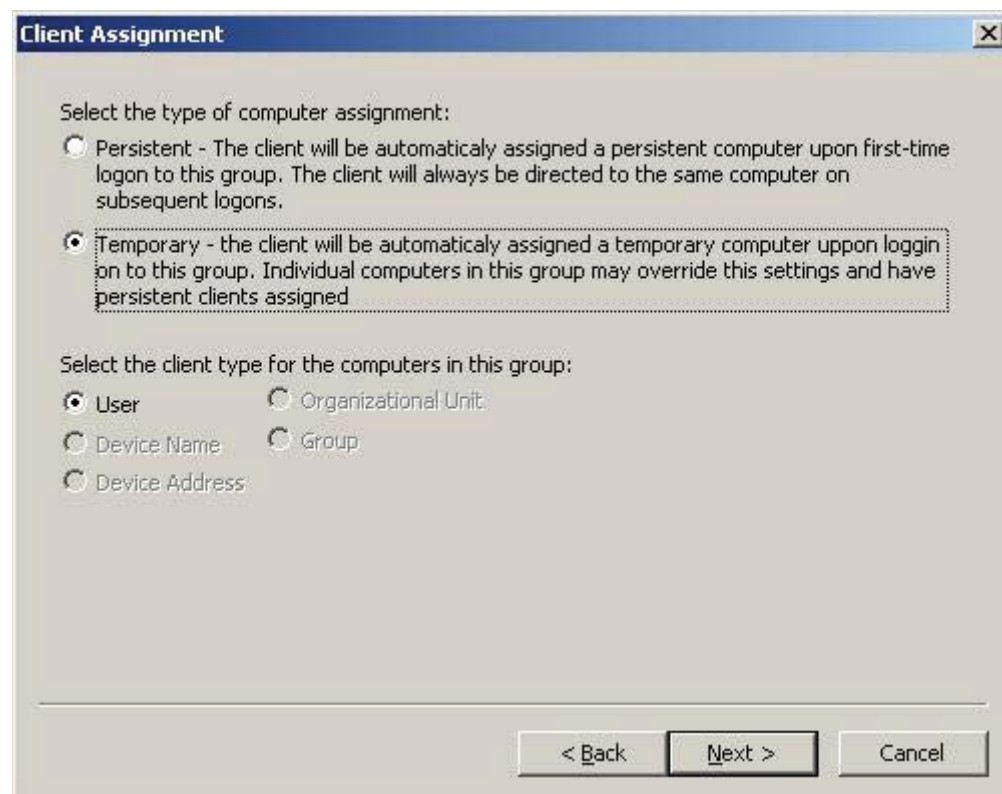
10. Enable/Disable Auto-Expand. Click *Next*

11. Select **Do nothing**. I will create or import computers later. Click **Finish** to complete the wizard

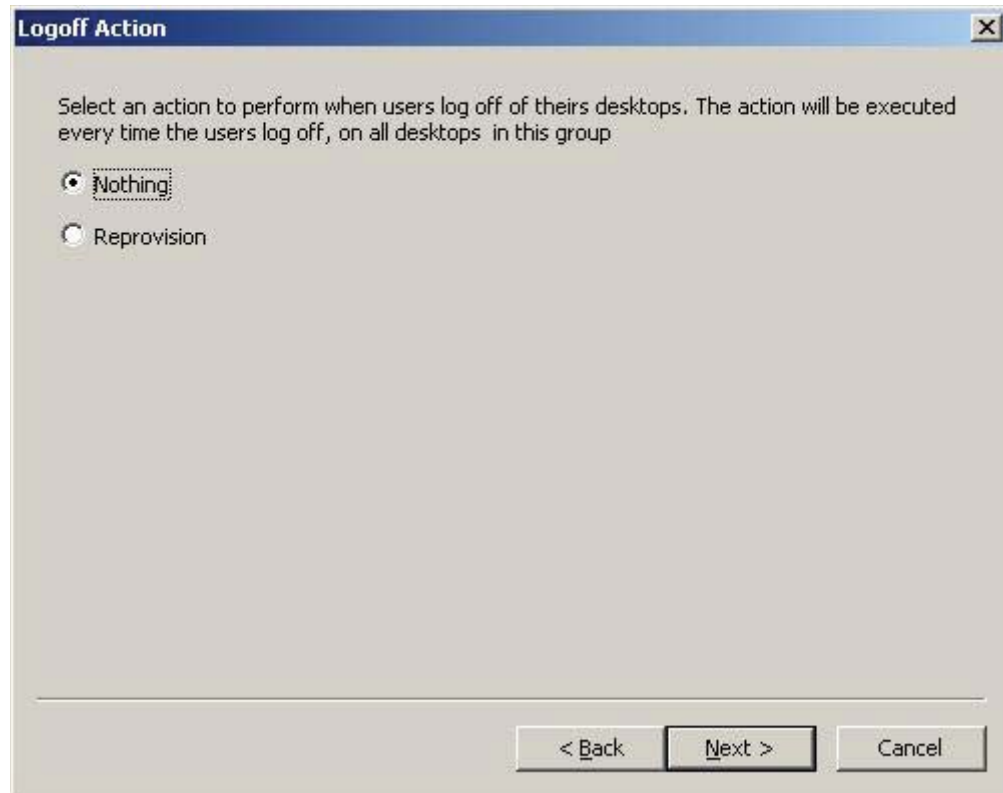
3.13.5 Create Temporary Desktop Group with No Logoff action for VDI

To create Temporary Desktop Group with No Logoff action for VDI:

1. Select **New Group** item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click **Next**
3. Select VDI hosting infrastructure for this group. Click **Next**
4. Select Datacenter from the list. Click **Next**
5. Specify Password for local Administrator. Click **Next**
6. Select **Temporary** type of Client Assignment. Click **Next**



7. Choose User Privileges. Click **Next**
8. Select process for Session Auto-Logoff or add new one. Click **Next**
9. Select **Nothing** Logoff action. Click **Next**



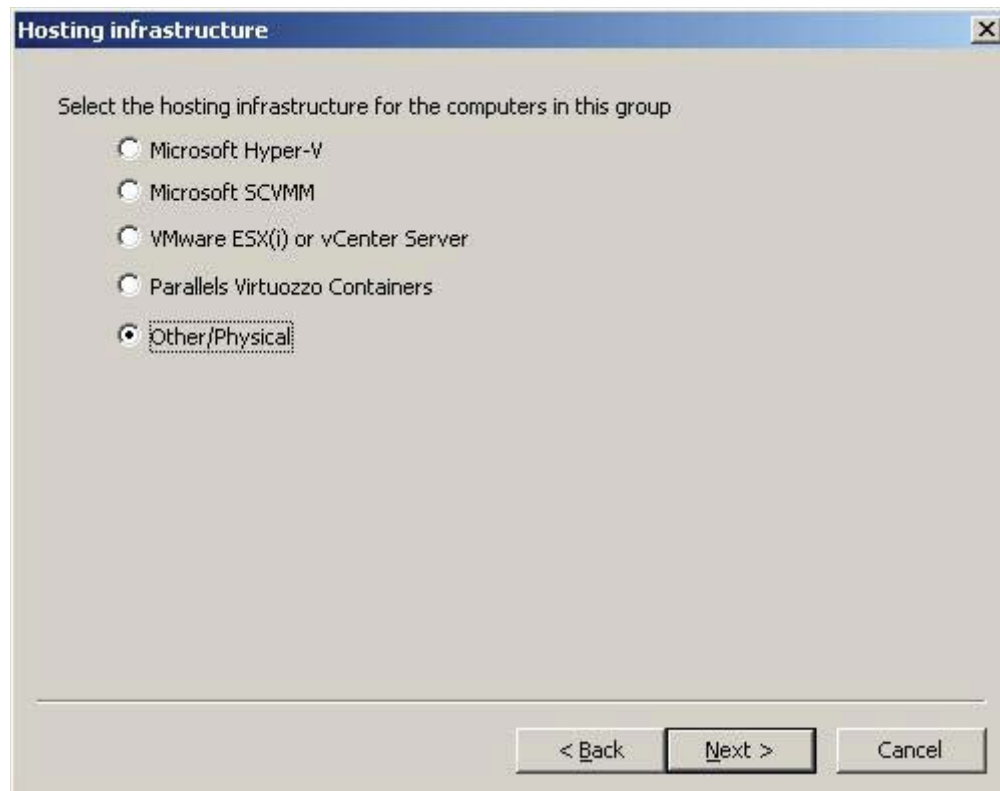
10. Enable/Disable Auto-Expand. Click *Next*

11. Select Do nothing. I will create or import computers later. Click *Finish* to complete the wizard

3.13.6 Create Temporary Desktop Group for Other/Physical

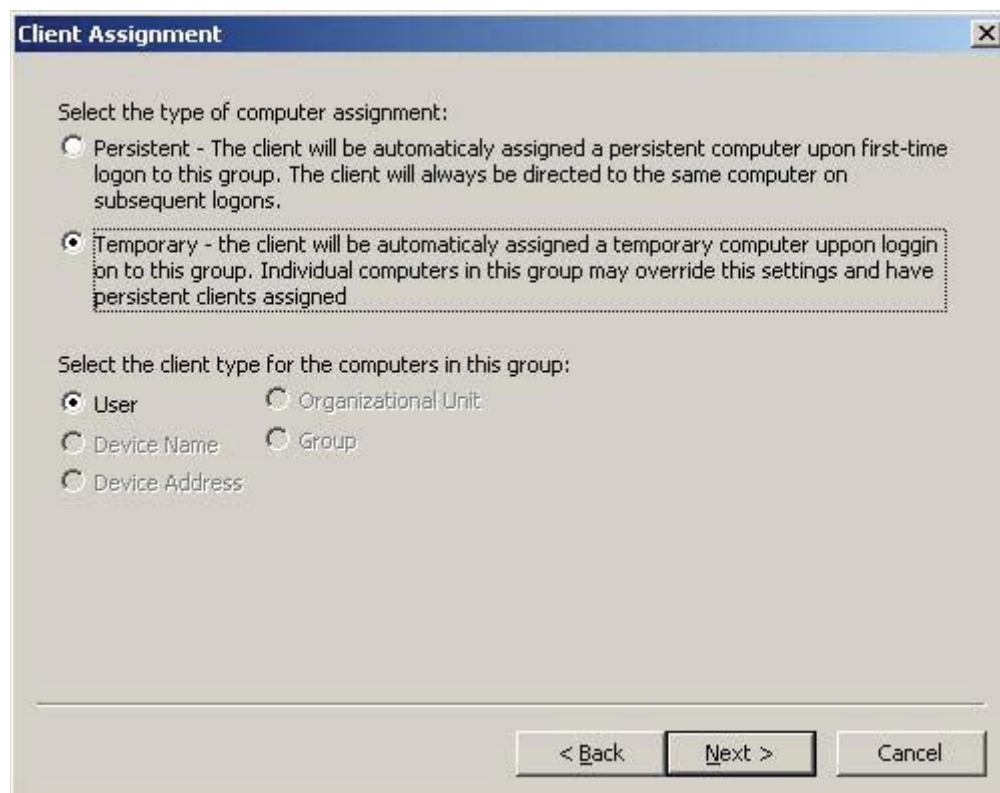
To create Temporary Desktop Group for Other/Physical:

1. Select *New Group* item from Desktop Groups right-click menu.
2. Enter friendly name for Desktop Group. Click *Next*
3. Select *Other/Physical* hosting infrastructure for this group. Click *Next*



4. Specify Password for local Administrator. Click *Next*

5. Select *Temporary* type of Client Assignment. Click *Next*



6. Choose User Privileges. Click *Next*

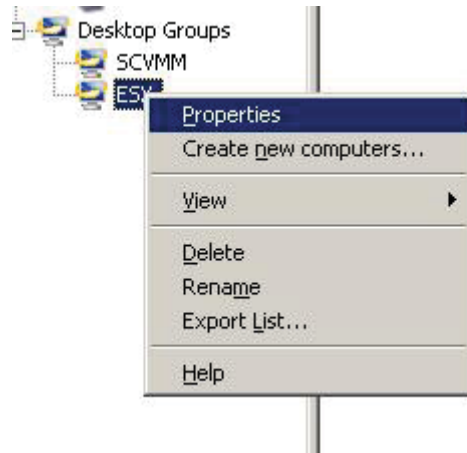
7. Select process for Session Auto-Logoff or add new one. Click *Next*

8. Select **Do nothing**. I will add computers later. Click **Finish** to complete the wizard

3.13.7 Modifying Desktop Group Properties

To modify Desktop Group properties:

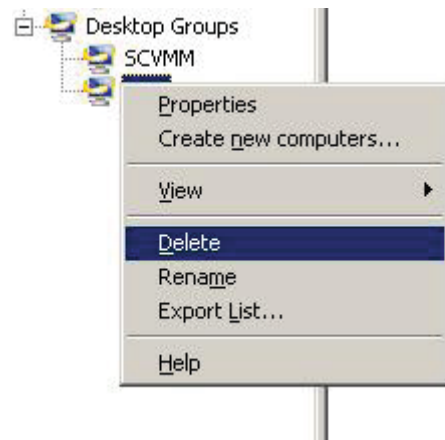
1. Select **Properties** item from Created Desktop Group right-click menu.



3.13.8 Deleting Desktop Group

To Delete Desktop Group from EMC.

1. Select **Delete** item from Created Desktop Groups right-click menu. **Confirmation window** appears.



2. Click **Yes** if you sure to delete this group.



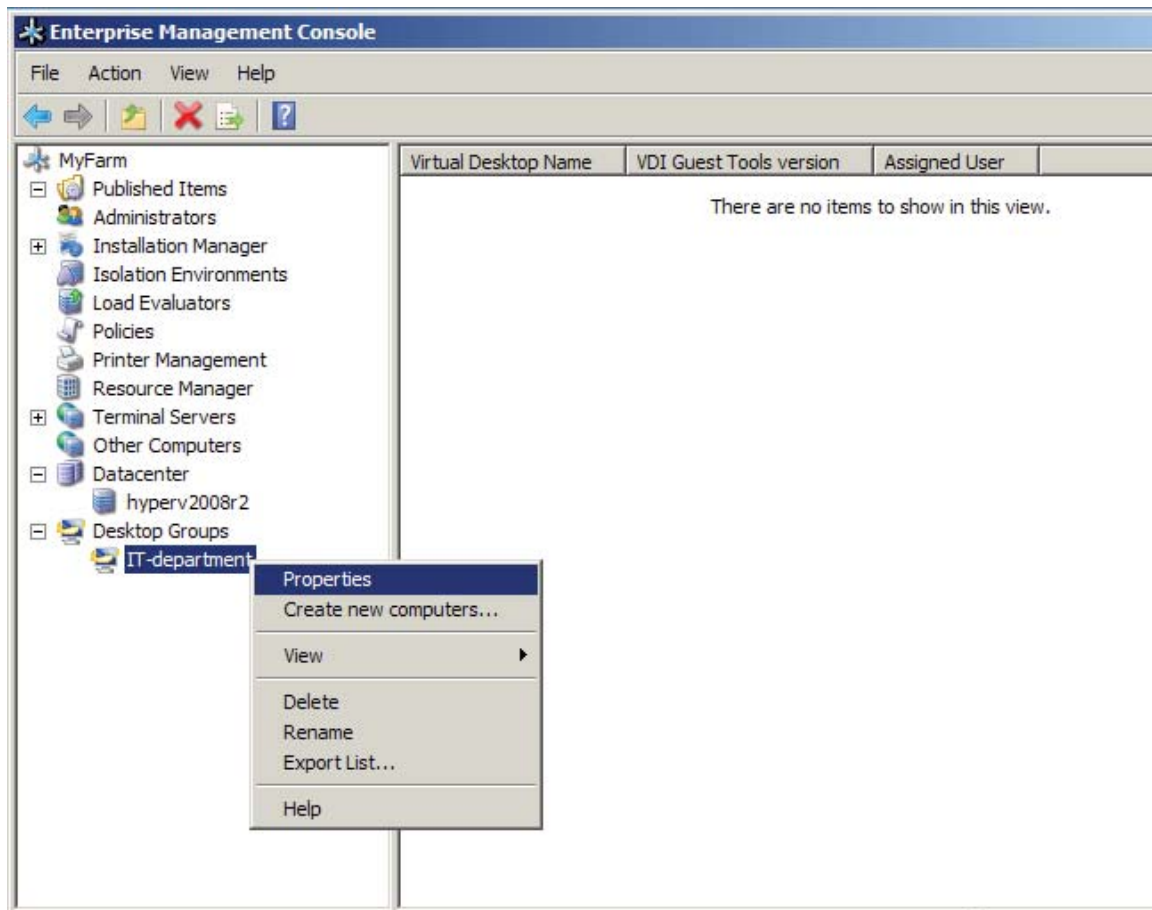
3.14 Managing Computers in Desktop Groups

3.14.1 Adding Computers to Desktop Groups

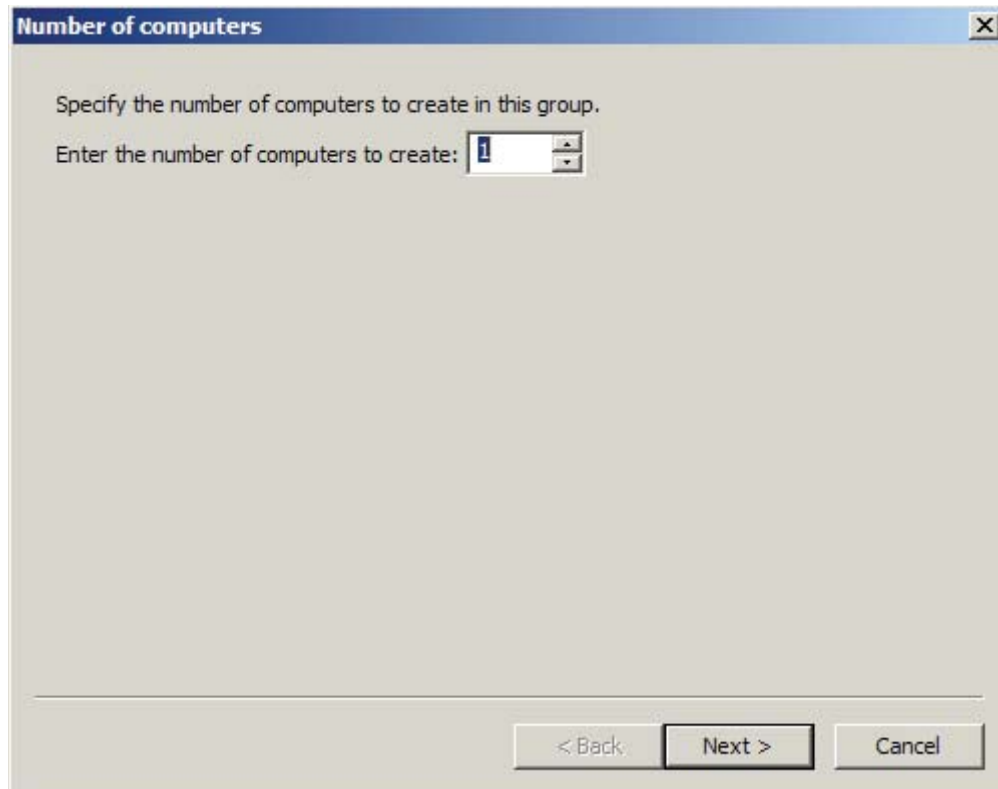
3.14.1.1 Add computer to Hyper-V Desktop Group

To create new computers to specific desktop group:

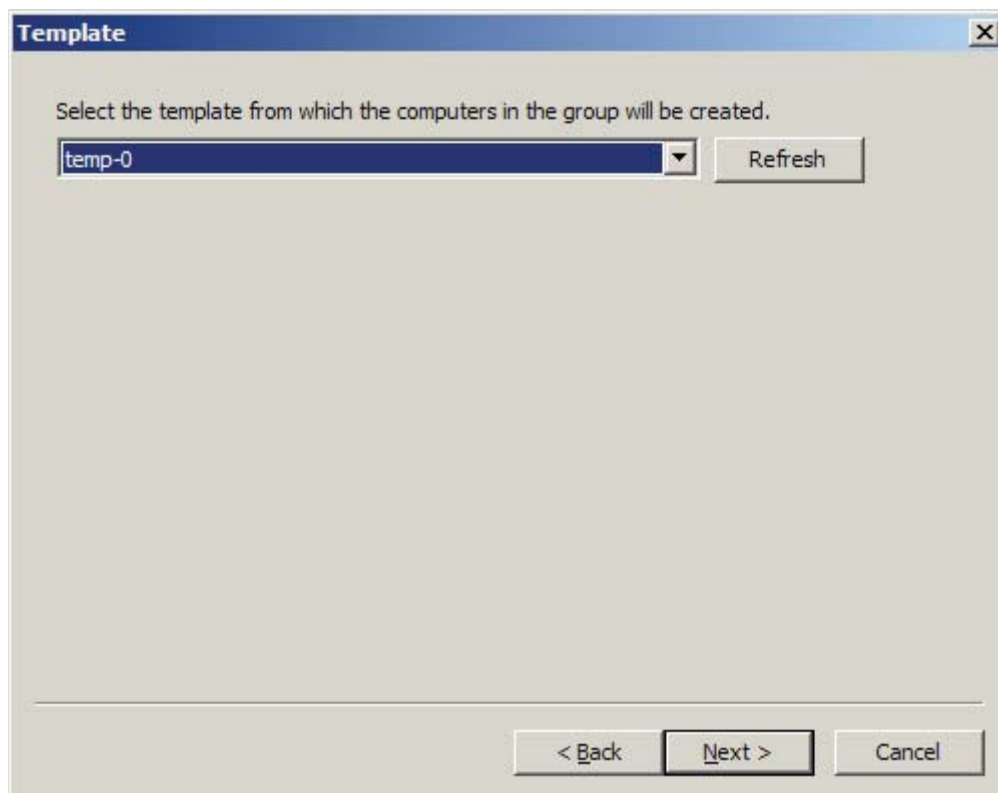
1. Select **Create new computers** item from right-click menu of specific desktop group.



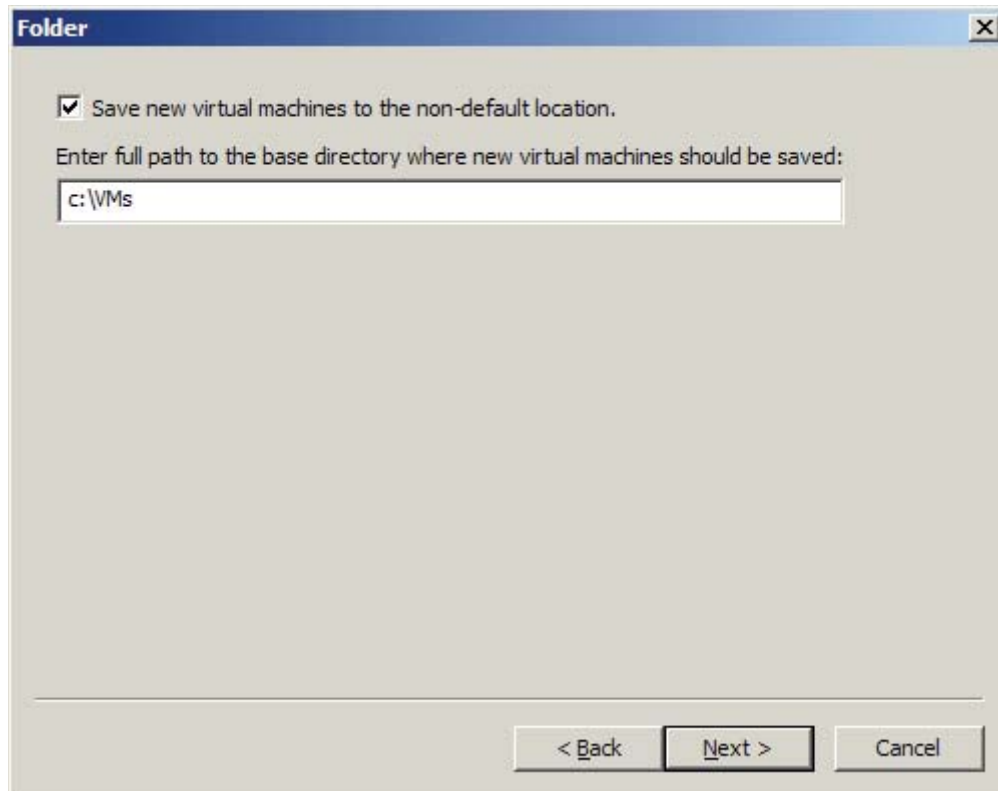
2. Specify the number of computers to create. Click **Next**



3. Then select a *Hyper-V* virtual machine, which will be used as a template for computers creation. Click *Next*

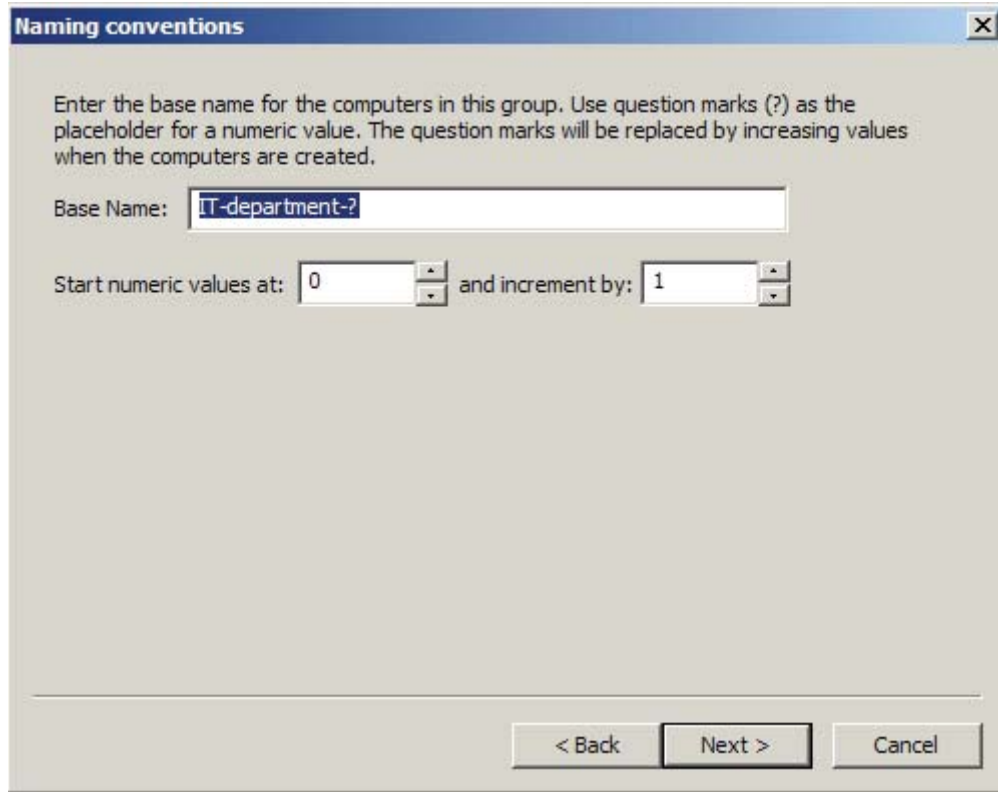


4. Select destination, where VM will be stored after creation. You can specify path manually. Or clone to default destination (where template VM is located). Click *Next*



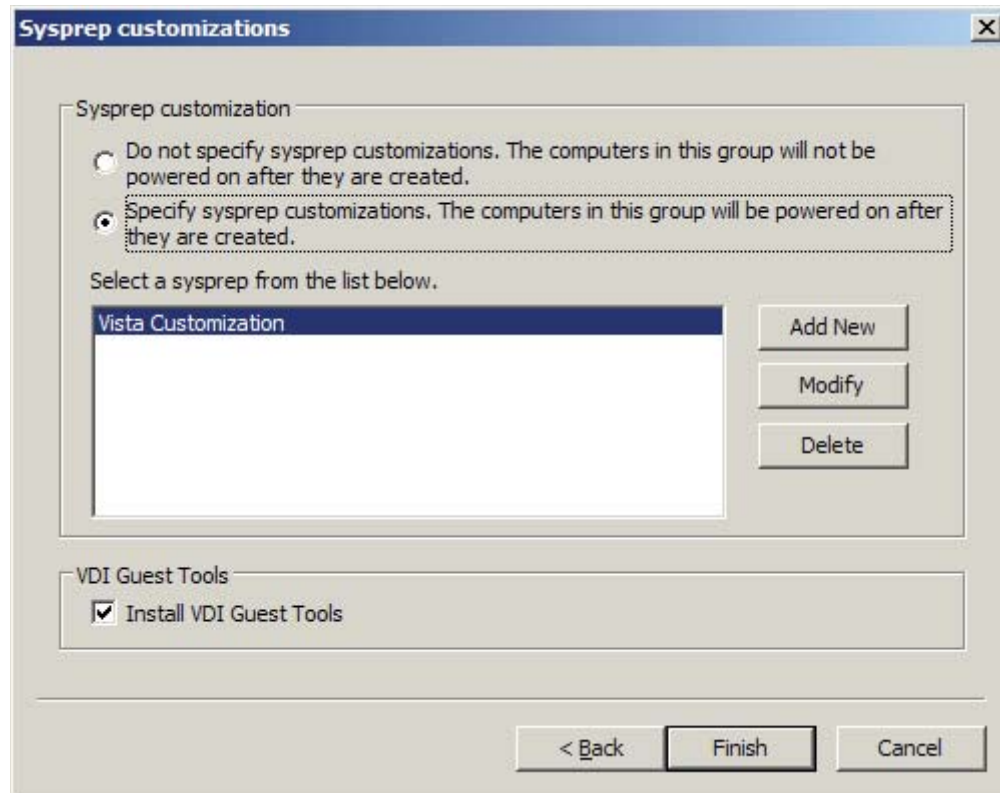
The 'Folder' dialog box has a title bar with a close button. It contains a checked checkbox labeled 'Save new virtual machines to the non-default location.' Below this is a text prompt: 'Enter full path to the base directory where new virtual machines should be saved:'. A text input field contains the path 'c:\VMs'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Specify the base name for computers in the group. Click *Next*



The 'Naming conventions' dialog box has a title bar with a close button. It contains a text prompt: 'Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.' Below this is a text input field for 'Base Name:' containing 'IT-department-?'. Underneath are two numeric input fields: 'Start numeric values at:' followed by a field containing '0', and 'and increment by:' followed by a field containing '1'. Both numeric fields have up and down arrow buttons. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

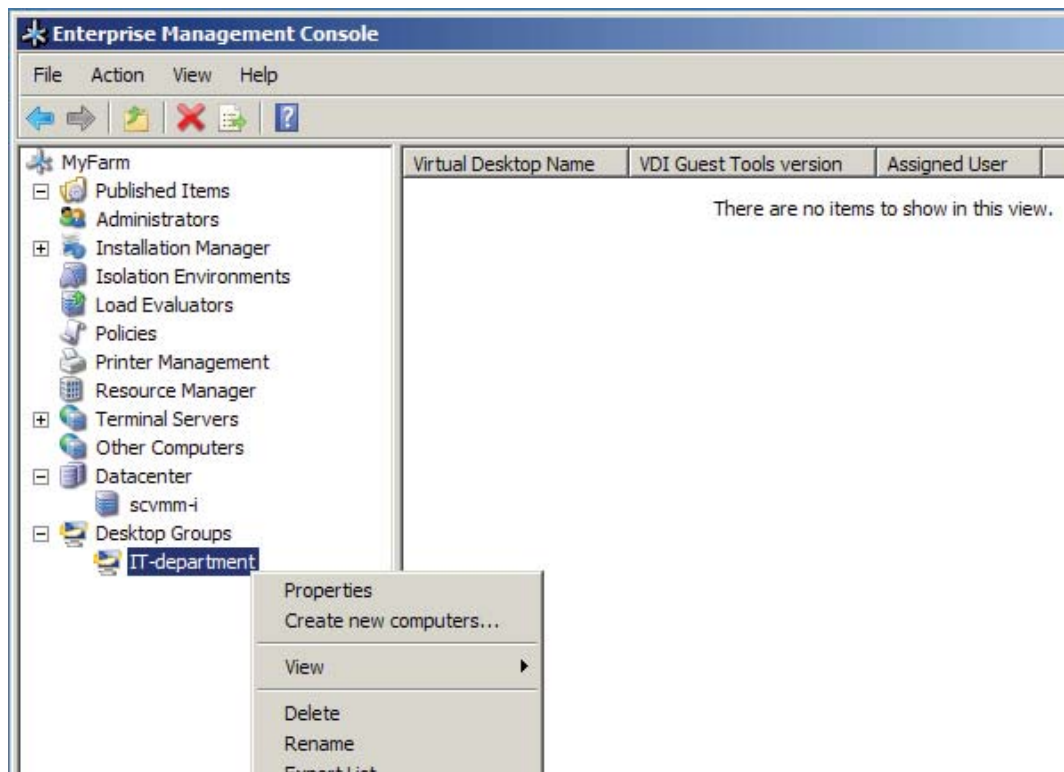
6. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click *Finish*



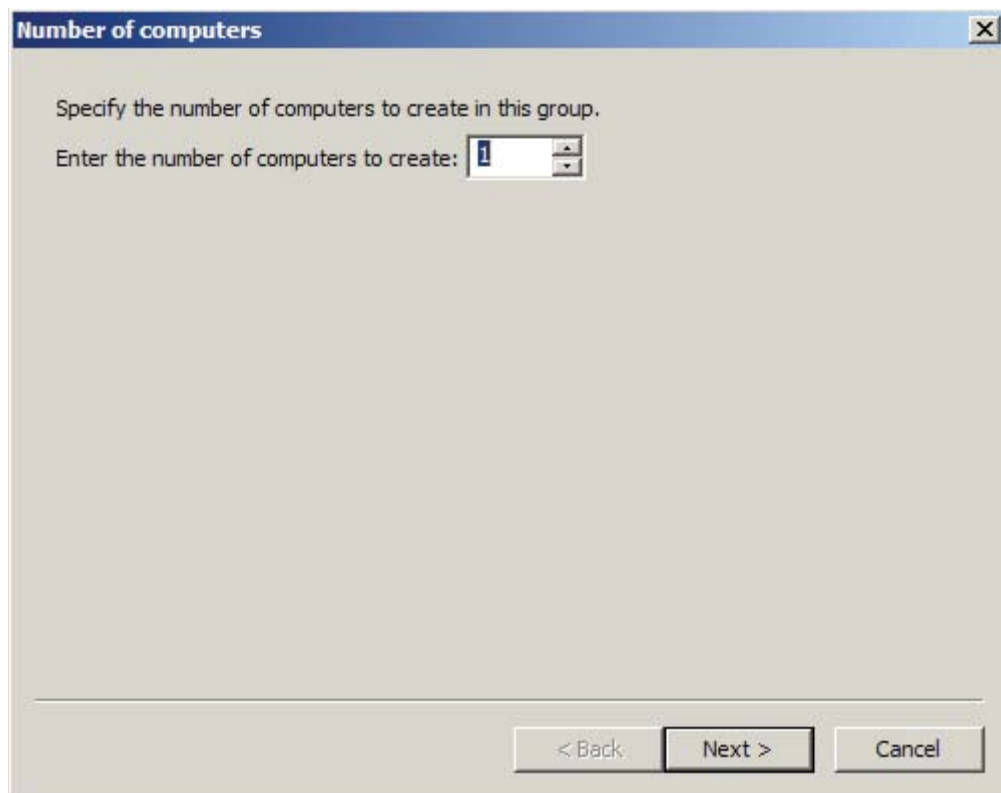
3.14.1.2 Add computer to SCVMM Desktop Group

To create new computers to specific desktop group:

1. Select **Create new computers** item from right-click menu of specific desktop group.

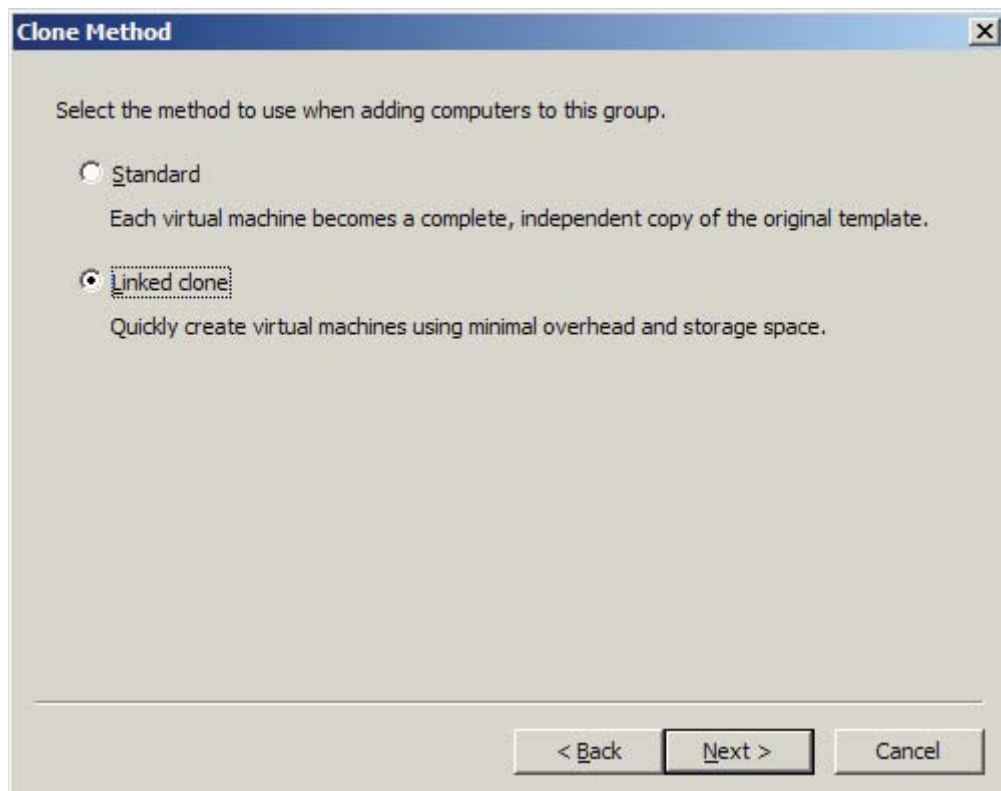


2. Specify the number of computers to create.



A dialog box titled "Number of computers" with a close button (X) in the top right corner. The text inside reads: "Specify the number of computers to create in this group." followed by "Enter the number of computers to create:". Below this text is a numeric input field with a spinner control, currently showing the value "1". At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

3. Choose clone method. There are two methods available for SCVMM datacenters:



A dialog box titled "Clone Method" with a close button (X) in the top right corner. The text inside reads: "Select the method to use when adding computers to this group." Below this text are two radio button options. The first option is "Standard", which is currently unselected. The second option is "Linked clone", which is selected. Below each option is a descriptive sentence. At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

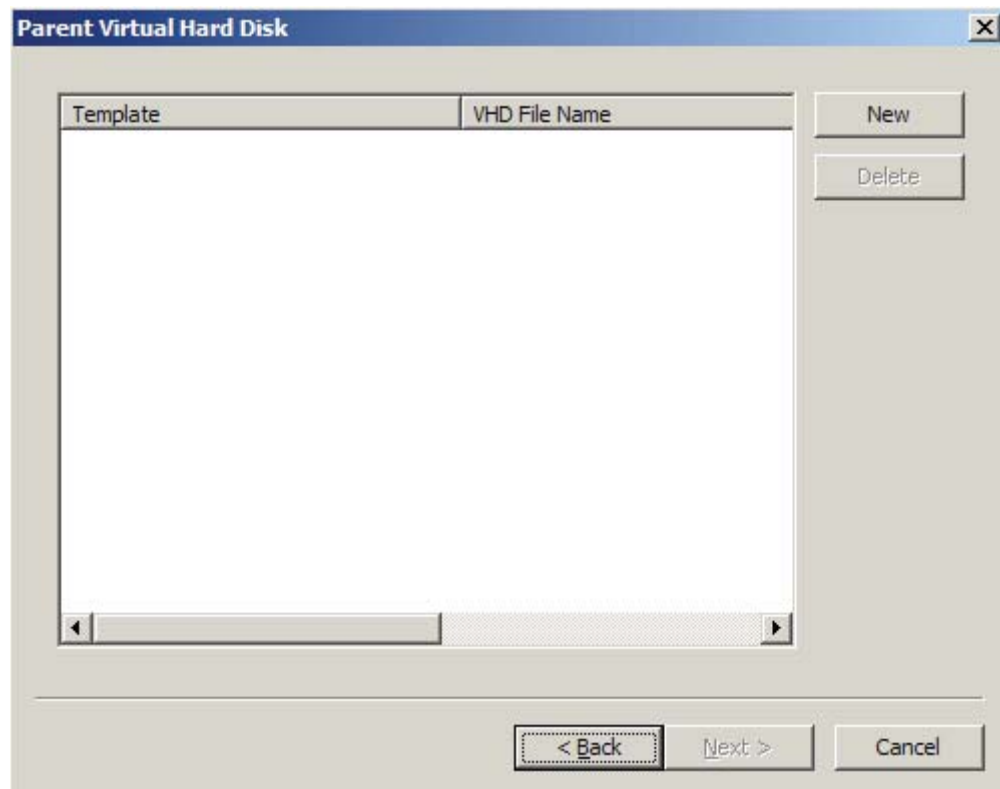
Standard - a standard clone is an independent copy of a virtual machine that

shares nothing with the parent virtual machine after the cloning operation. On-going operation of a standard clone is entirely separate from the parent virtual machine. Standard clones take longer to create than linked clones

Linked – a linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation.

For Linked clone:

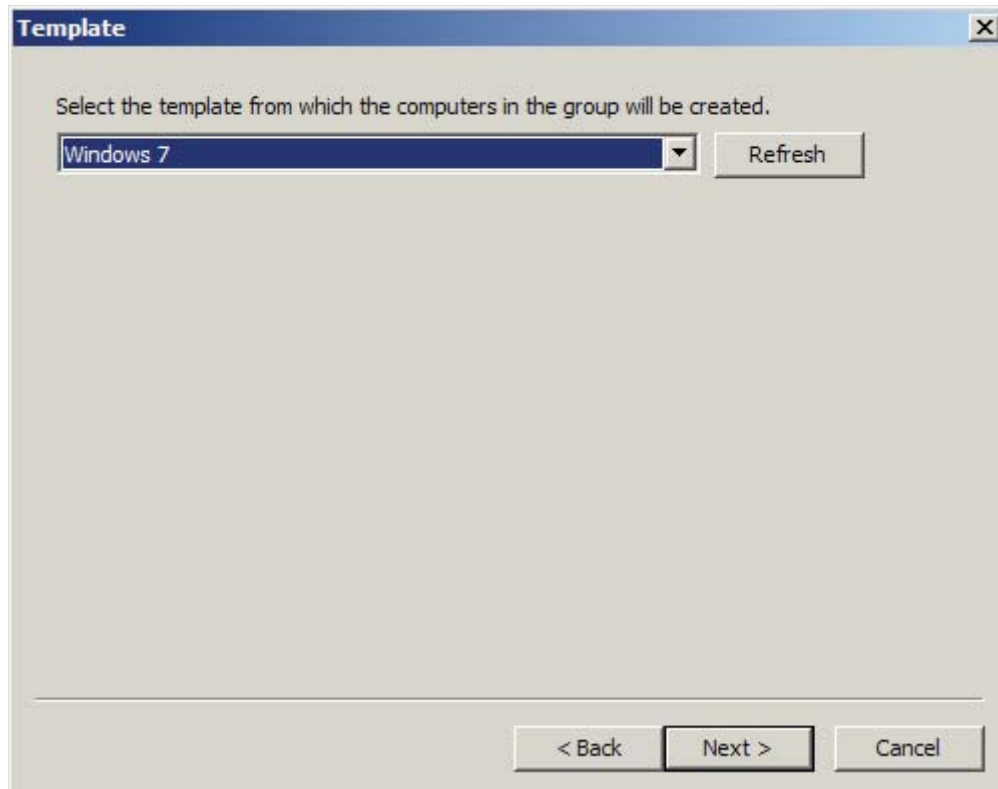
4. Create Parent Virtual Hard Disk.



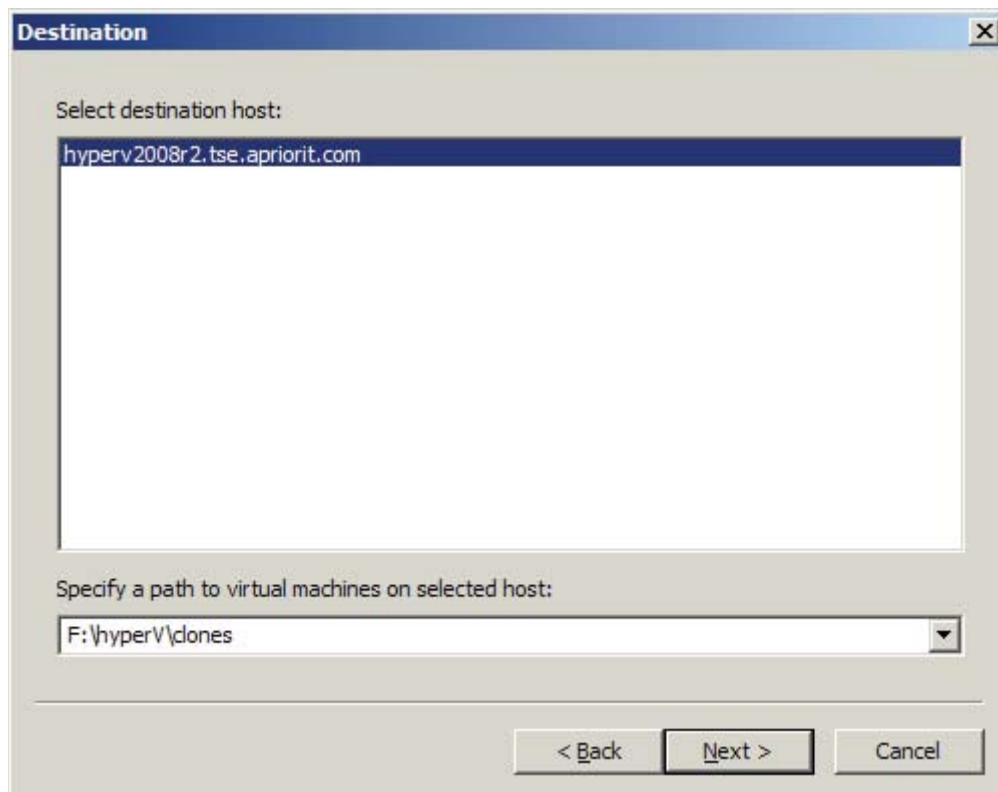
To create Parent Virtual Hard Disk:

4.1 Click **New** to create Parent VHD.

4.2 Select template for Parent VHD. Click **Next**

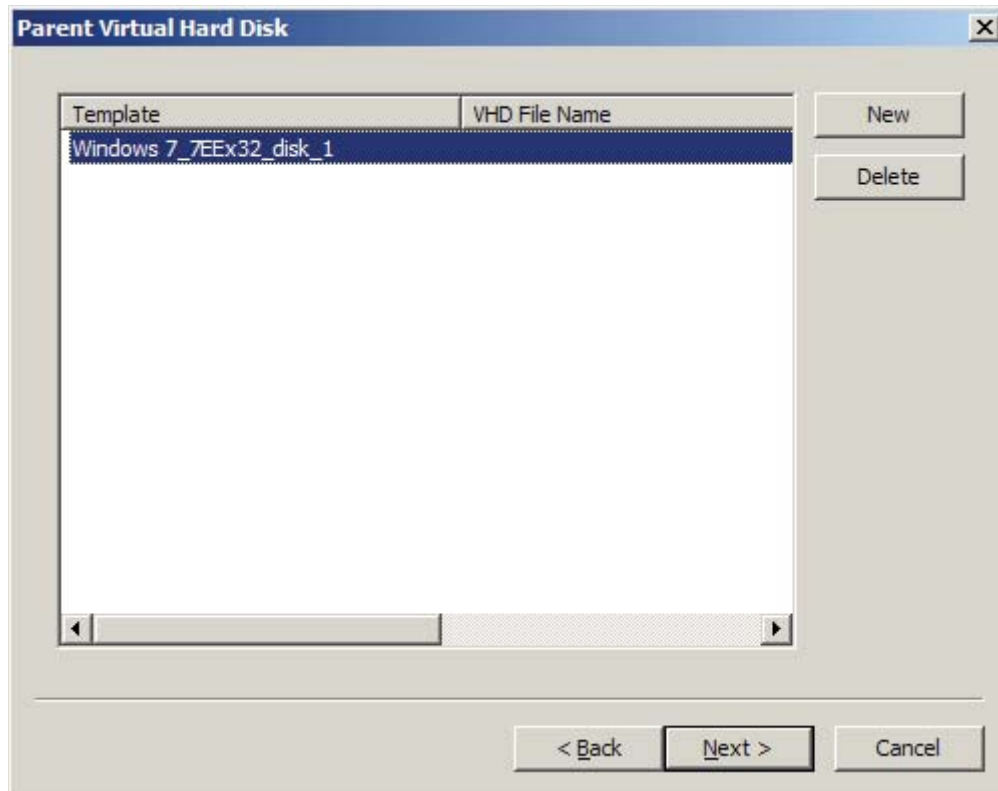


4.3 Specify path on hypervisor to store Parent VHD. Click *Finish*

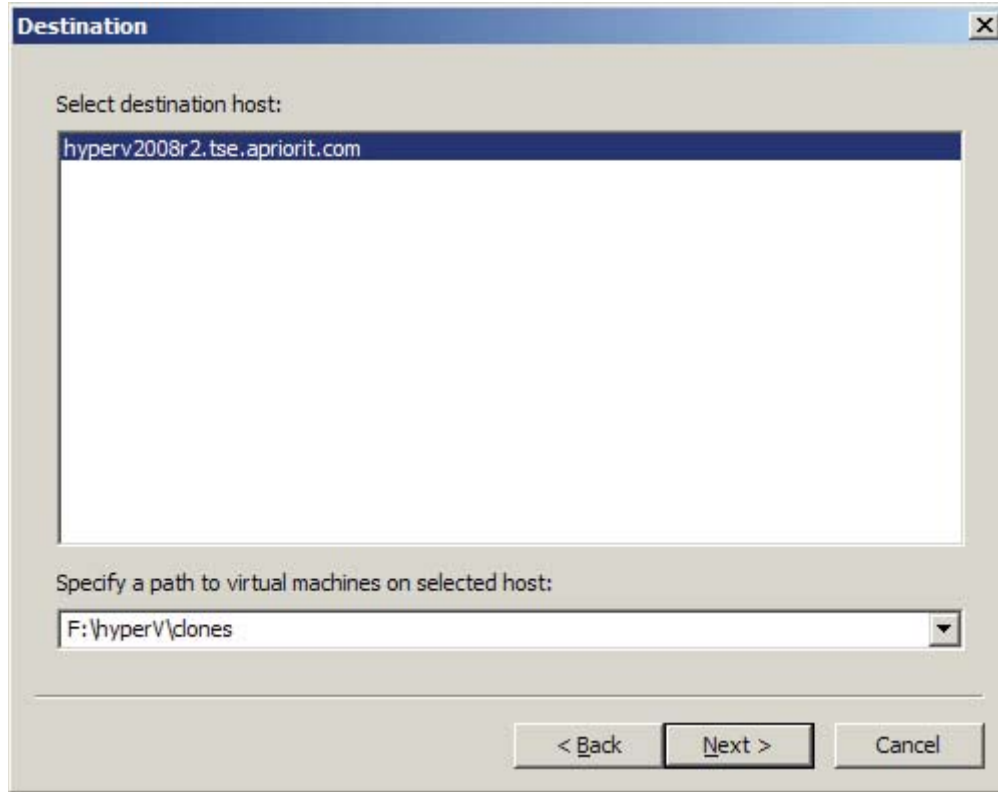


Created Parent VHD is displayed. We can reuse it during creation VMs with linked clone method.

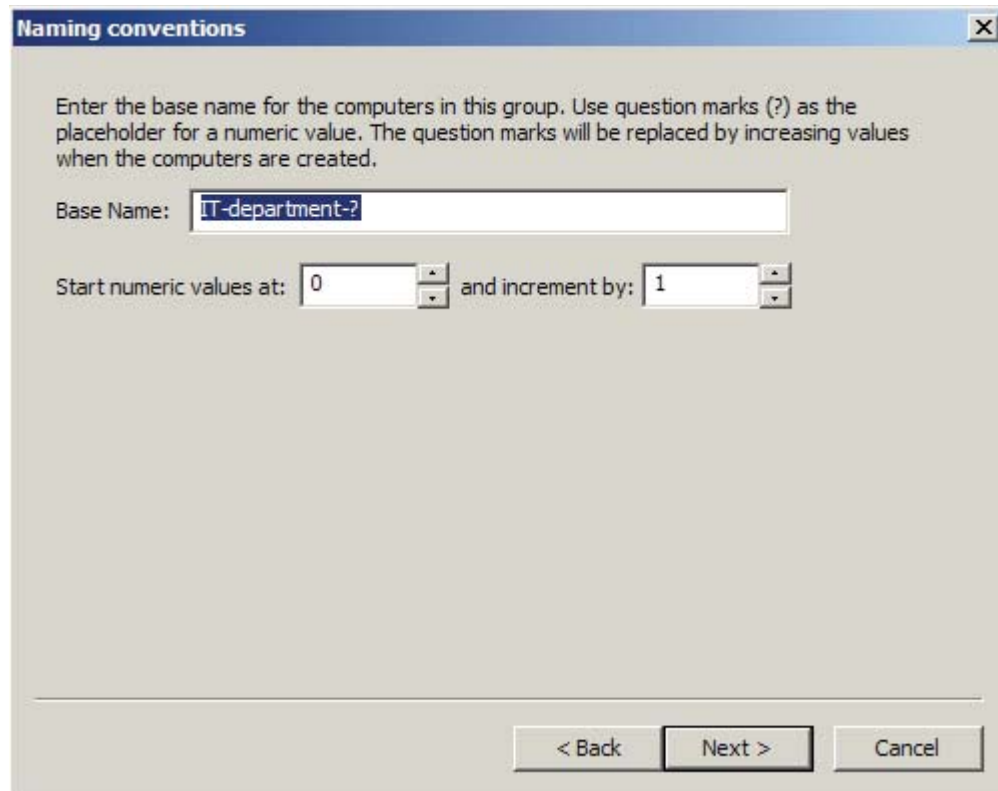
5. Select Created Parent VHD. Click *Next*



6. Specify place to store cloned VMs. Click *Next*



7. Specify the base name for computers in the group.



Naming conventions

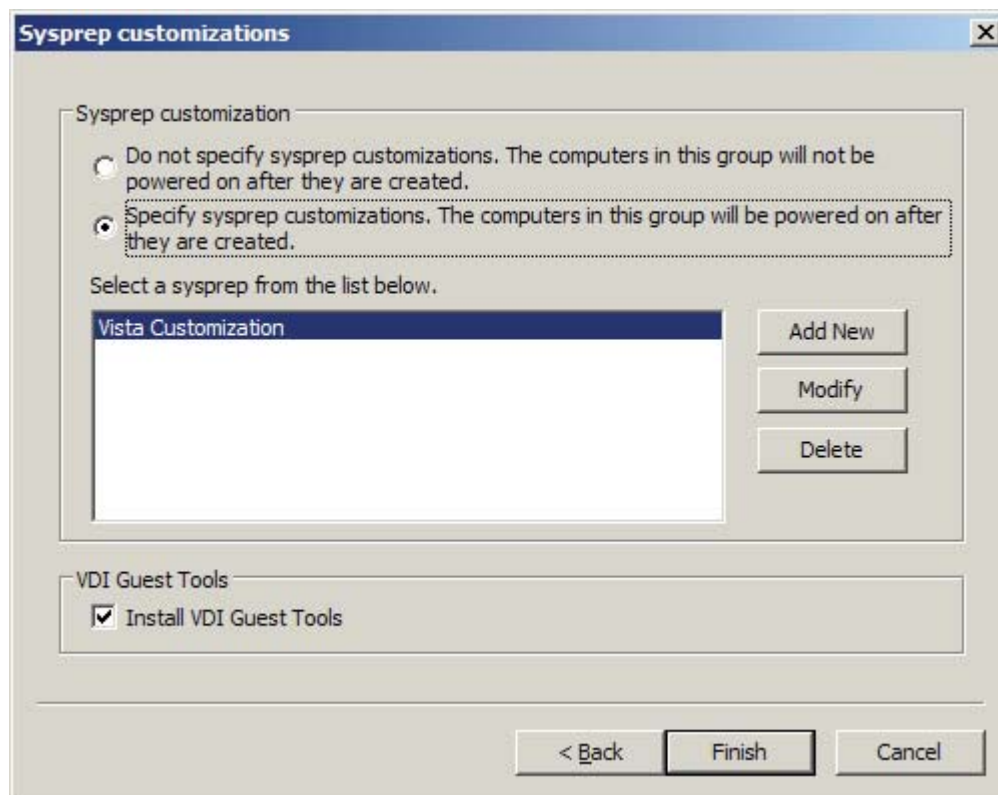
Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.

Base Name:

Start numeric values at: and increment by:

< Back Next > Cancel

8. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click **Finish**



Sysprep customizations

Sysprep customization

☐ Do not specify sysprep customizations. The computers in this group will not be powered on after they are created.

☒ Specify sysprep customizations. The computers in this group will be powered on after they are created.

Select a sysprep from the list below.

Vista Customization

Add New Modify Delete

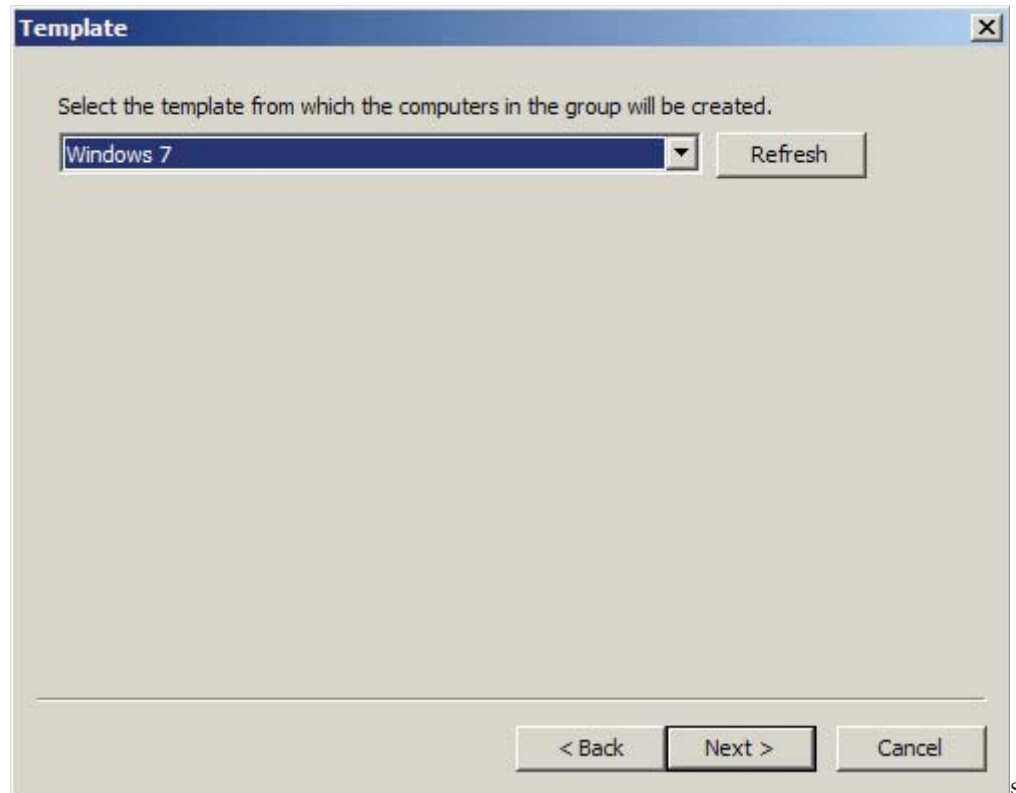
VDI Guest Tools

☒ Install VDI Guest Tools

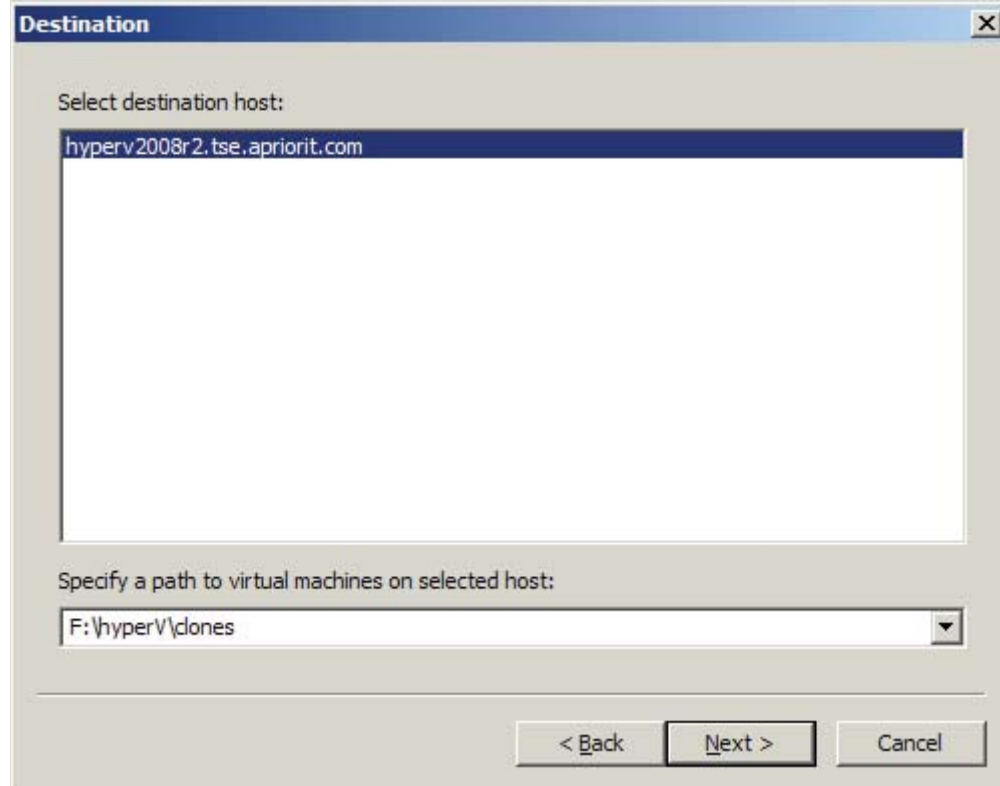
< Back Finish Cancel

For Standard clone:

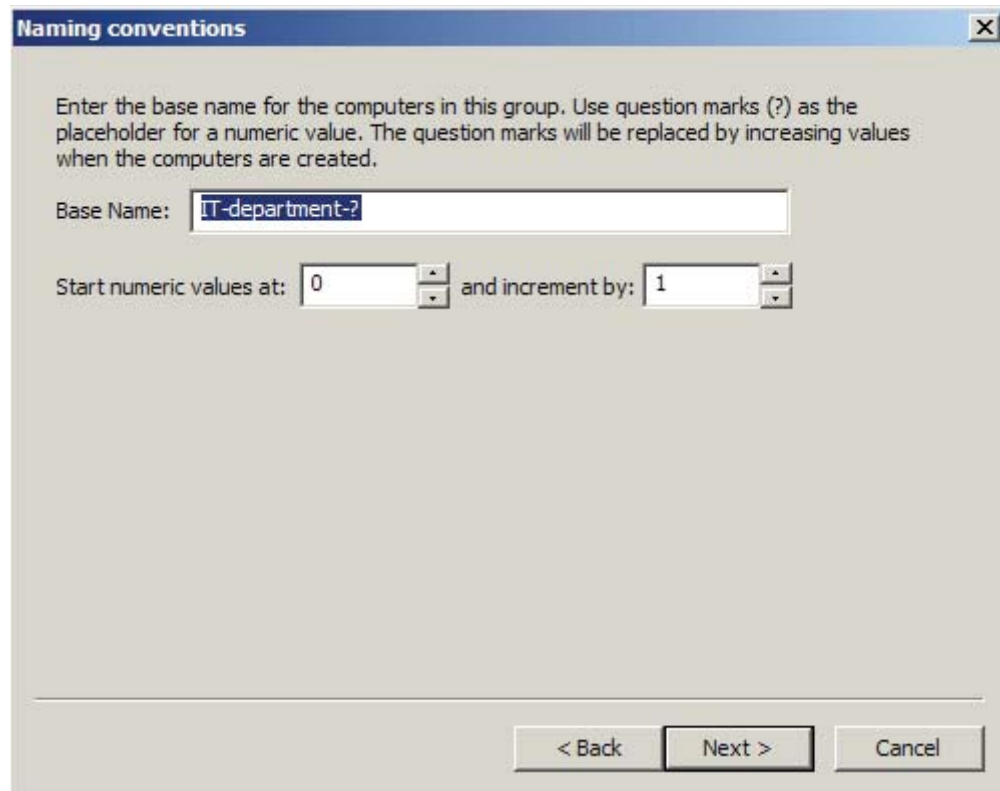
4. Select a template for computers creation. Click **Next**



5. Specify place to store cloned VMs. Click *Next*



6. Specify the base name for computers in the group.



Naming conventions

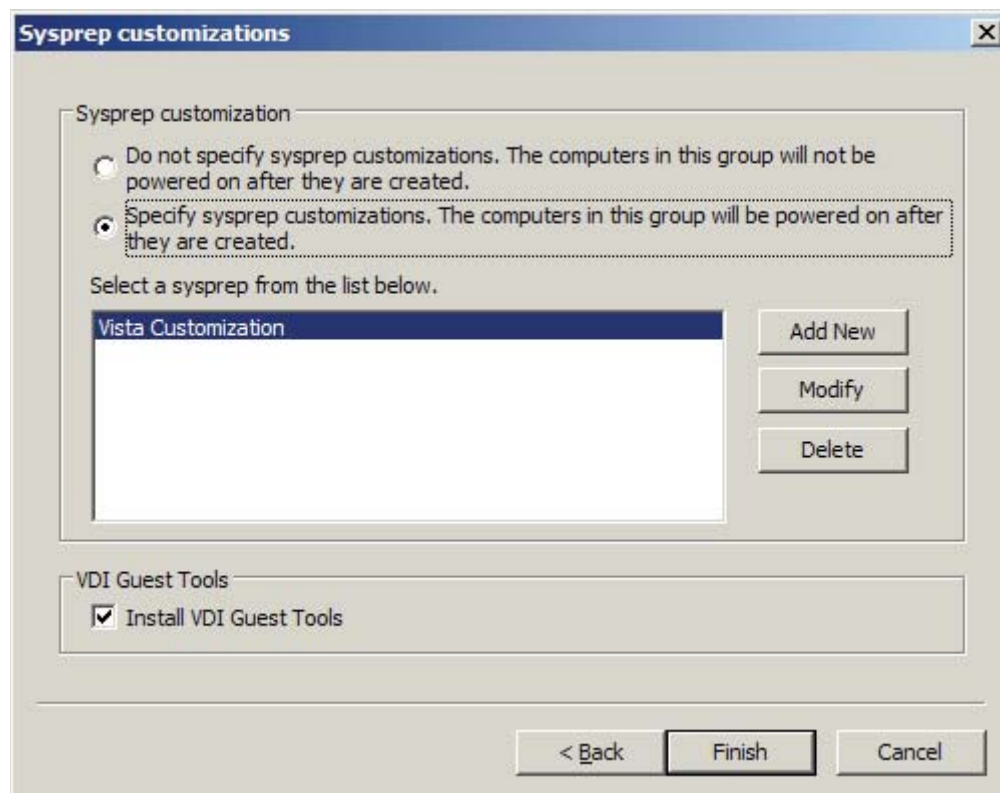
Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.

Base Name:

Start numeric values at: and increment by:

< Back Next > Cancel

7. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click **Finish**



Sysprep customizations

Sysprep customization

☐ Do not specify sysprep customizations. The computers in this group will not be powered on after they are created.

☒ Specify sysprep customizations. The computers in this group will be powered on after they are created.

Select a sysprep from the list below.

Vista Customization

Add New Modify Delete

VDI Guest Tools

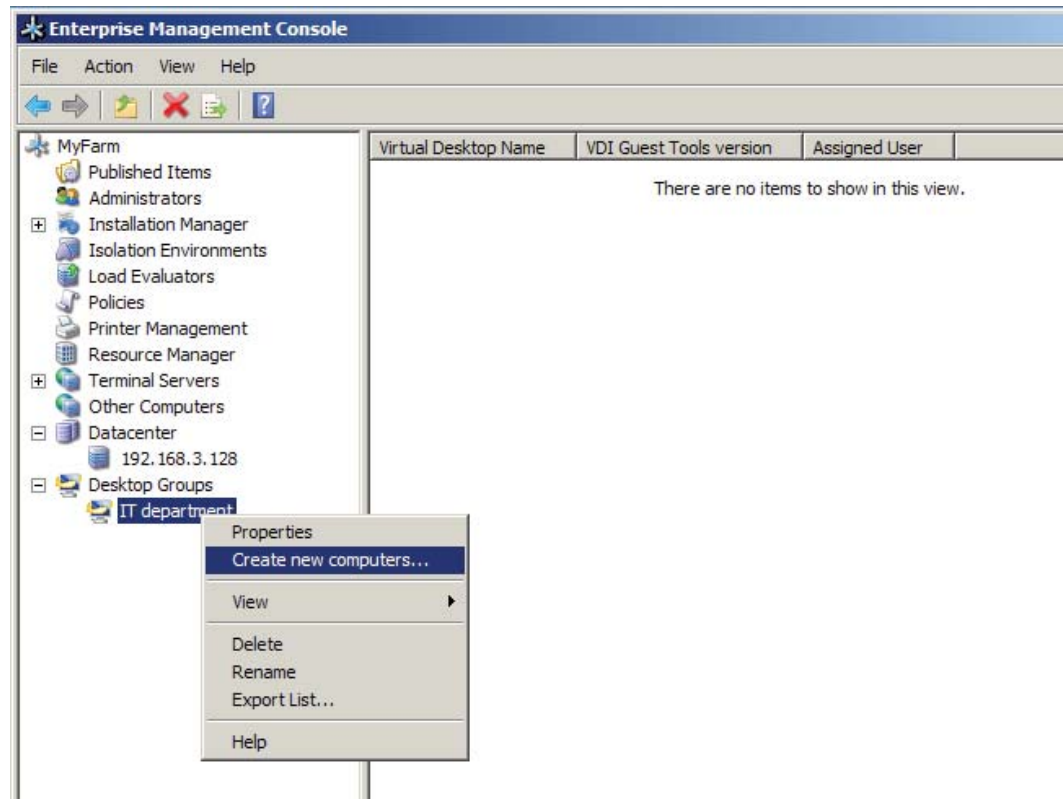
☒ Install VDI Guest Tools

< Back Finish Cancel

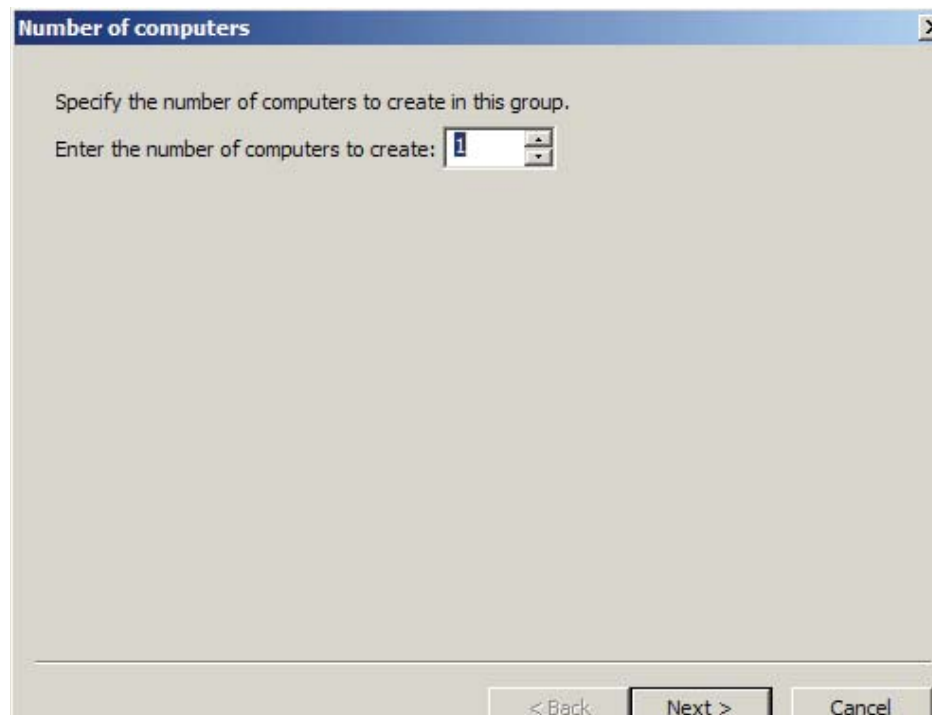
3.14.1.3 Add computer to ESX Desktop Group

To create new computers to specific desktop group:

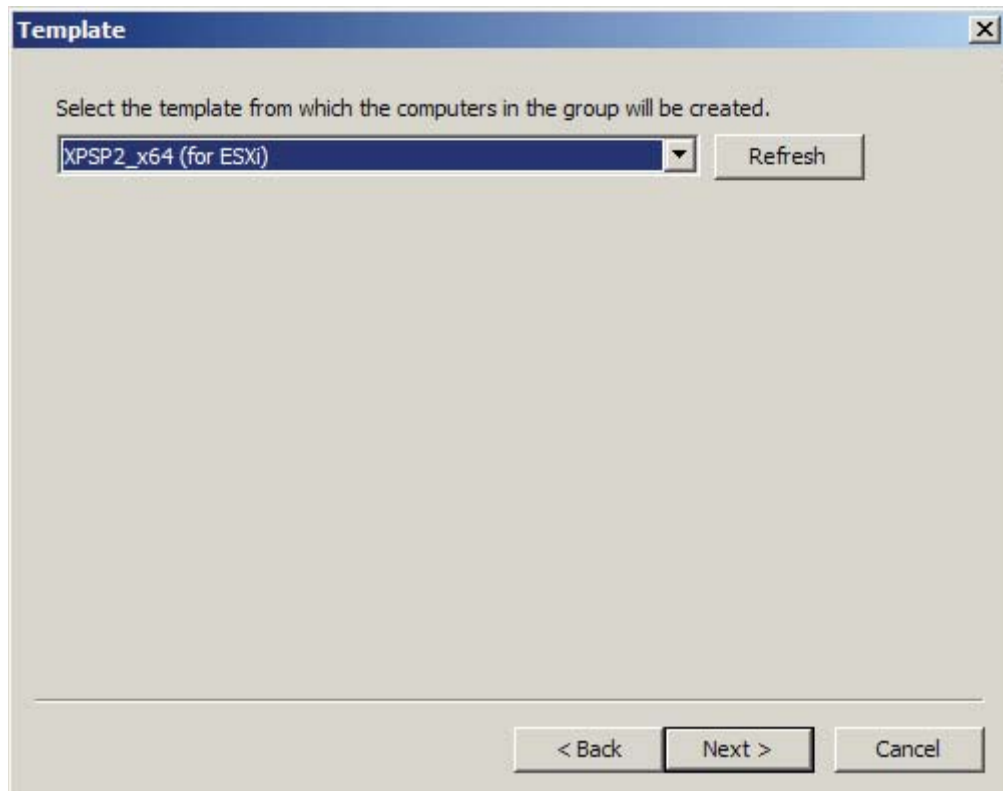
1. Select **Create new computers** item from right-click menu of specific desktop group.



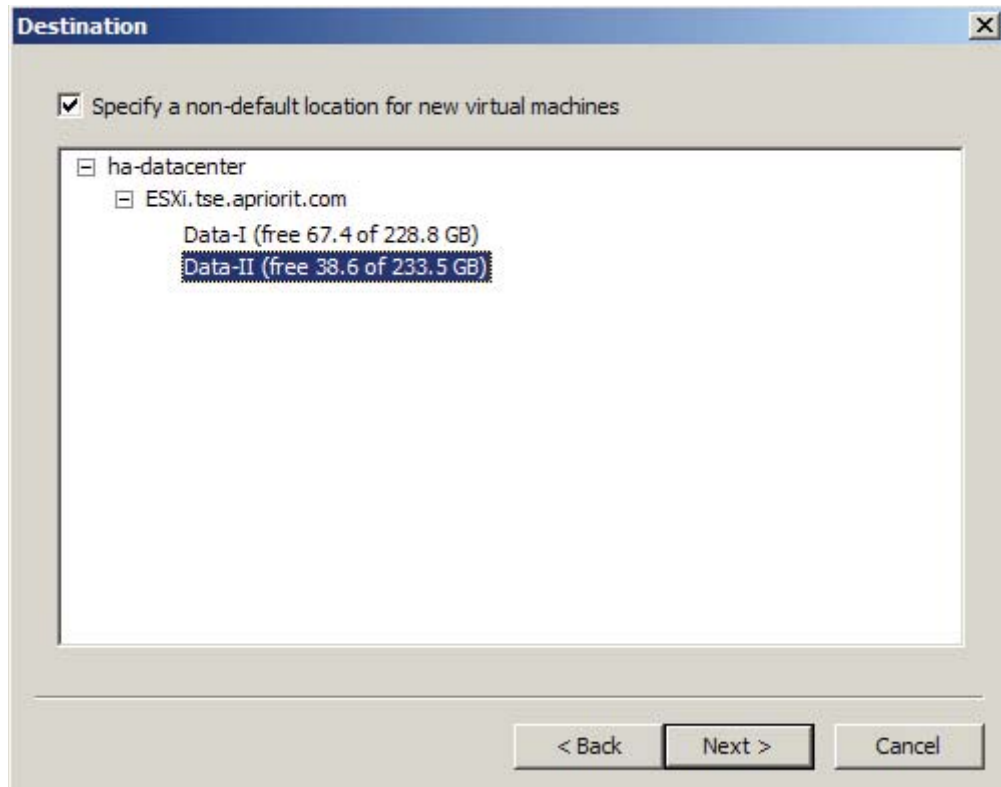
2. Specify the number of computers to create. Click **Next**



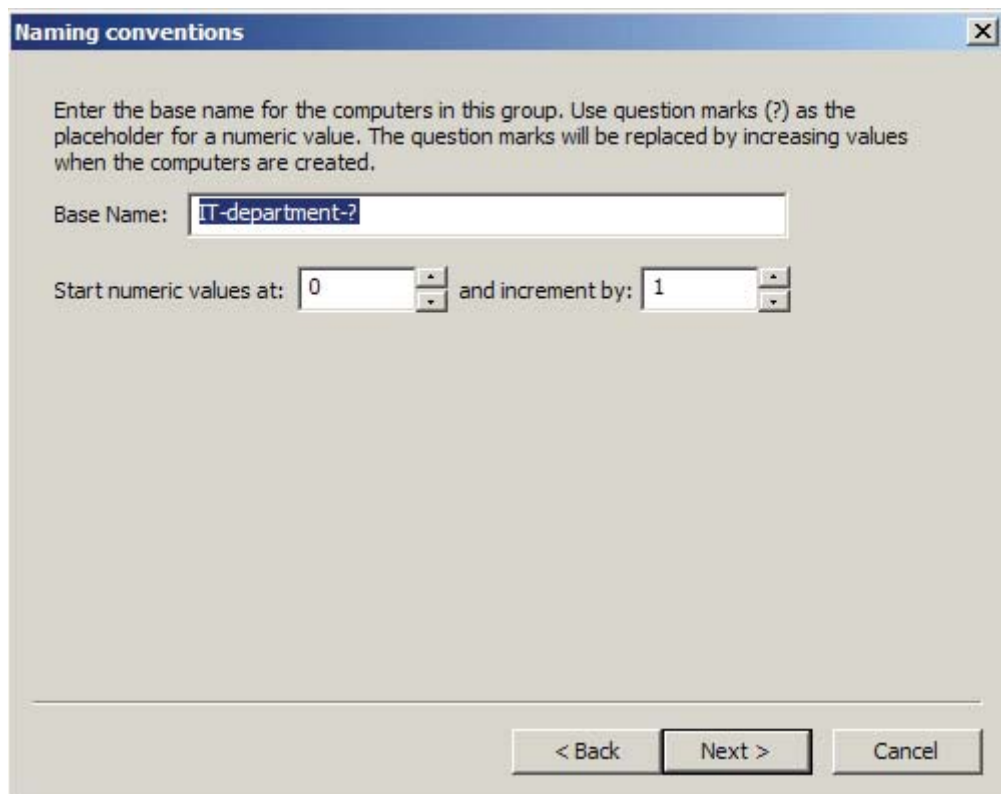
3. Select a **ESXi** virtual machine, which will be used as a template for computers creation. Click **Next**



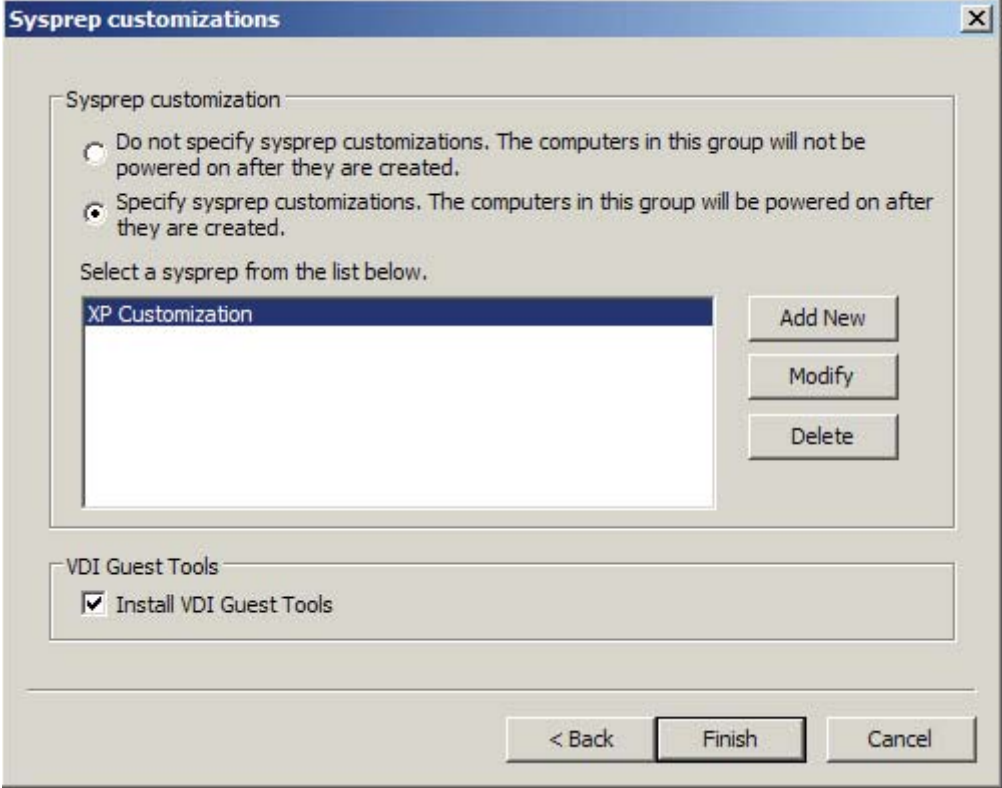
4. Select destination, where VM will be stored after creation. You can select ESXi datastore from list of available. Or clone to default destination (where template VM is located). Click **Next**



5. Specify the base name for computers in the group. Click *Next*



6. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click *Finish*



The image shows a Windows-style dialog box titled "Sysprep customizations". It contains two main sections. The first section, "Sysprep customization", has two radio buttons: "Do not specify sysprep customizations. The computers in this group will not be powered on after they are created." and "Specify sysprep customizations. The computers in this group will be powered on after they are created." The second radio button is selected. Below this is the text "Select a sysprep from the list below." followed by a list box containing "XP Customization". To the right of the list box are three buttons: "Add New", "Modify", and "Delete". The second section, "VDI Guest Tools", has a checked checkbox labeled "Install VDI Guest Tools". At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

Sysprep customizations

Sysprep customization

☐ Do not specify sysprep customizations. The computers in this group will not be powered on after they are created.

☒ Specify sysprep customizations. The computers in this group will be powered on after they are created.

Select a sysprep from the list below.

XP Customization

Add New

Modify

Delete

VDI Guest Tools

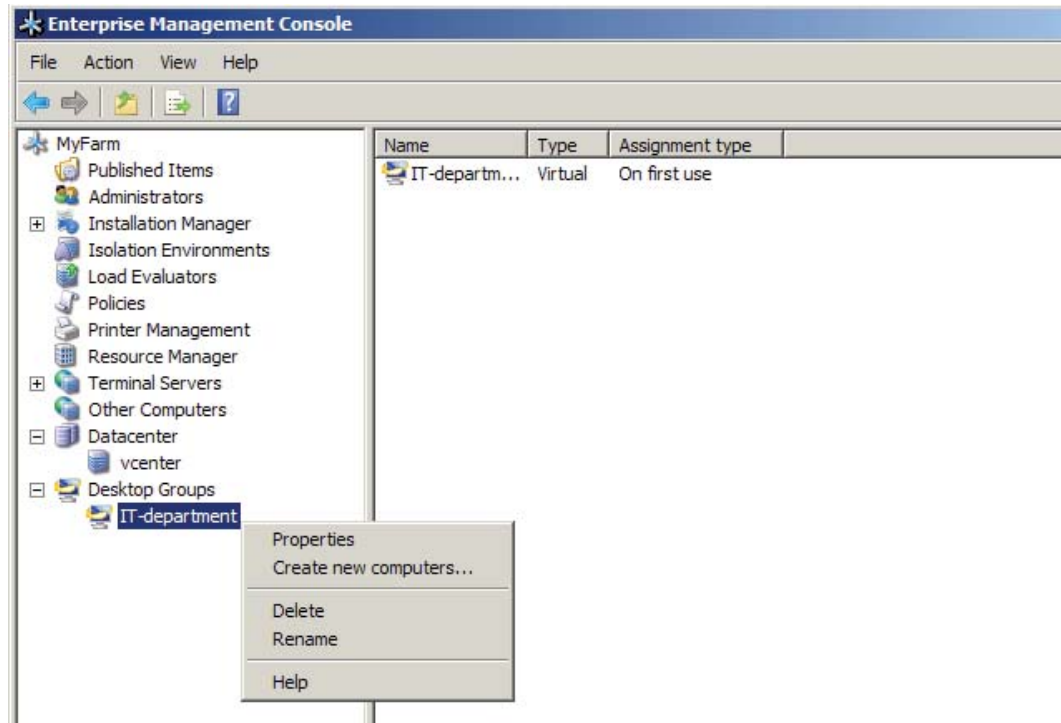
☒ Install VDI Guest Tools

< Back Finish Cancel

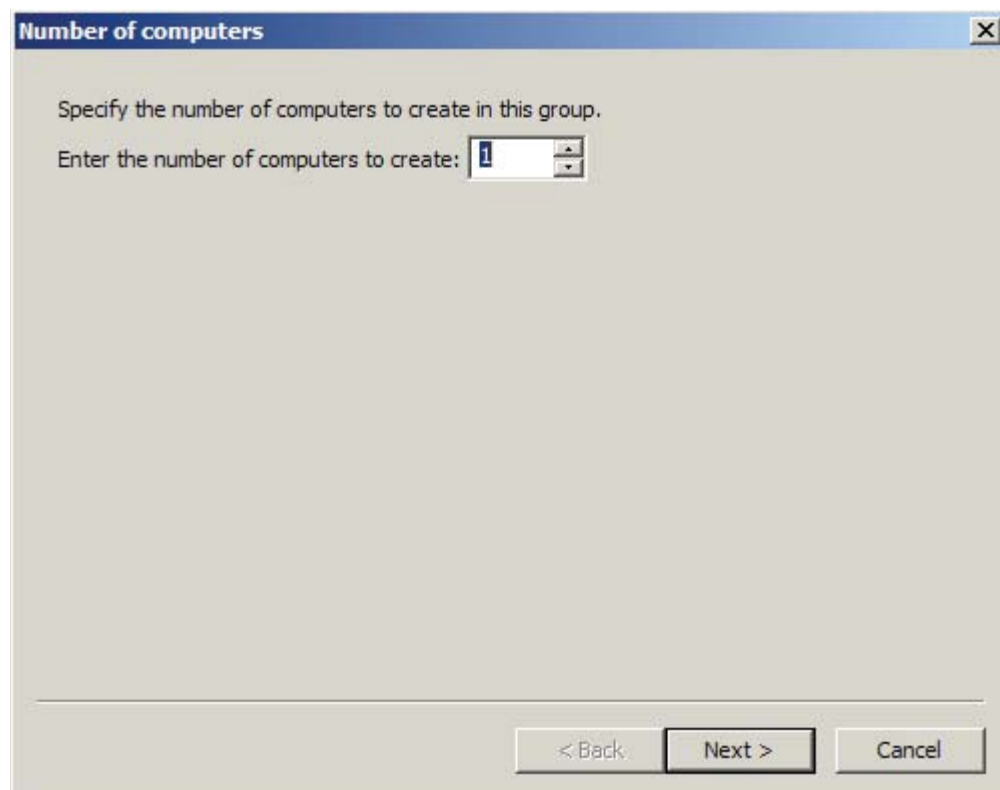
3.14.1.4 Add computer to vCenter Desktop Group

To create new computers to specific desktop group:

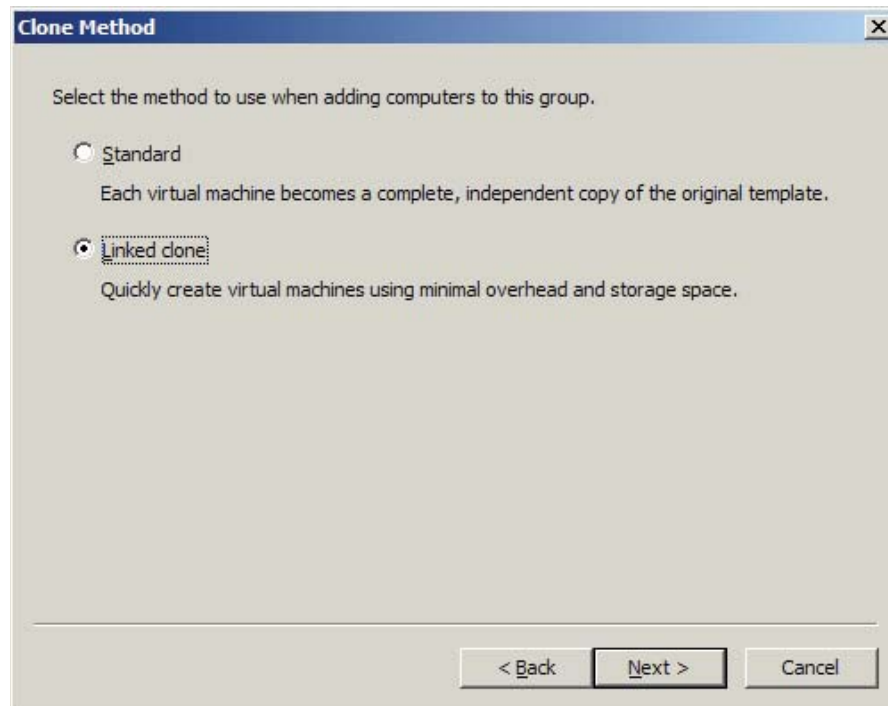
1. Select **Create new computers** item from right-click menu of specific desktop group.



2. Specify the number of computers to create.



3. Choose clone method. There are two methods available for SCVMM datacenters:

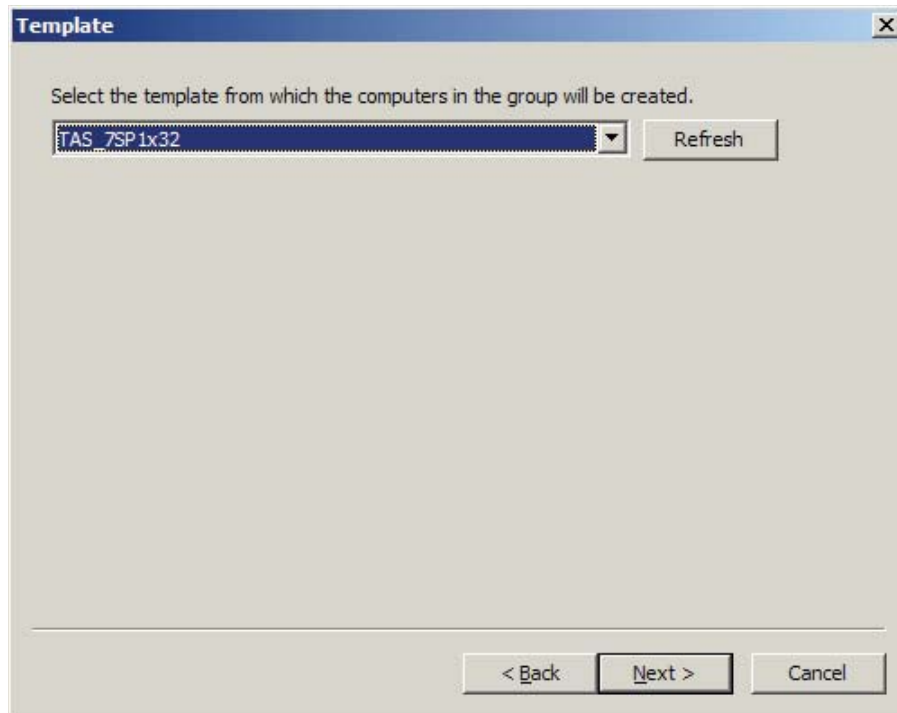


Standard - a standard clone is an independent copy of a virtual machine that shares nothing with the parent virtual machine after the cloning operation. On-going operation of a standard clone is entirely separate from the parent virtual machine. Standard clones take longer to create than linked clones

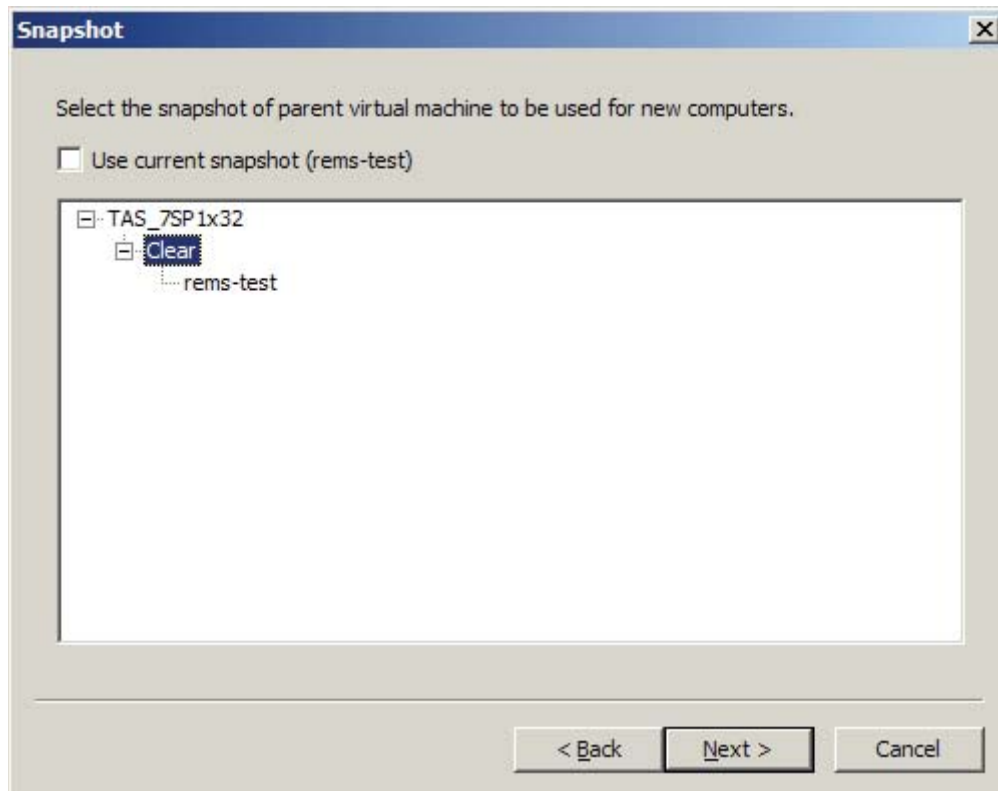
Linked - a linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation.

For Linked clone:

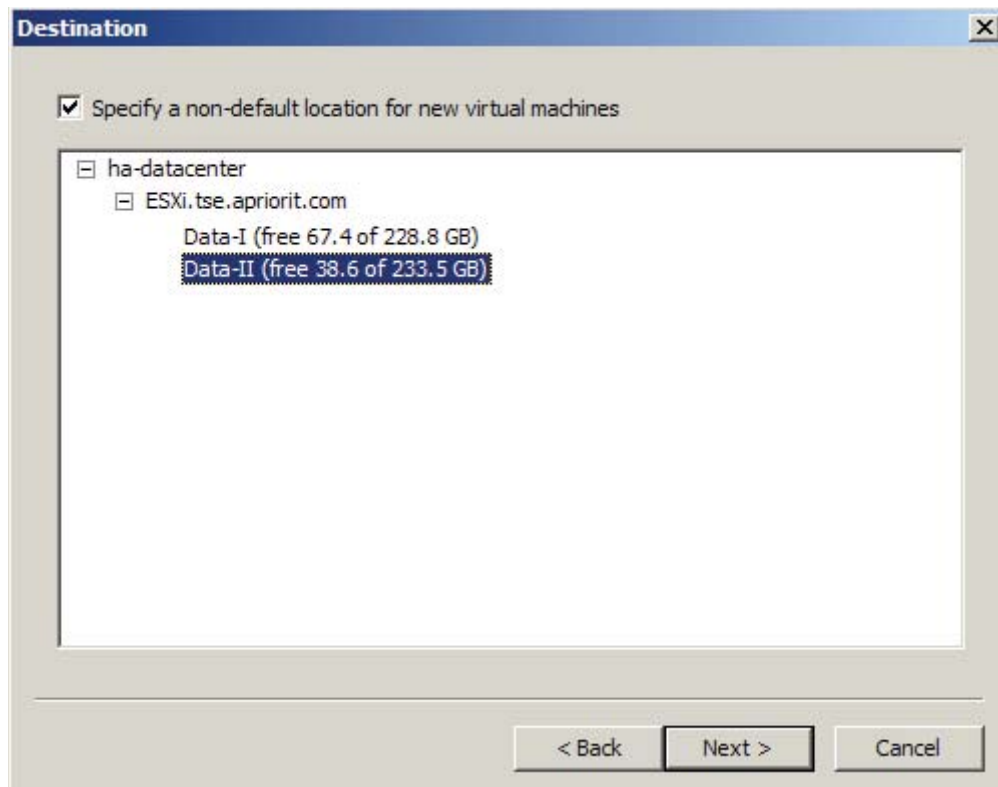
4. Select a **vCenter** virtual machine, which will be used as a template for computers creation. Click **Next**



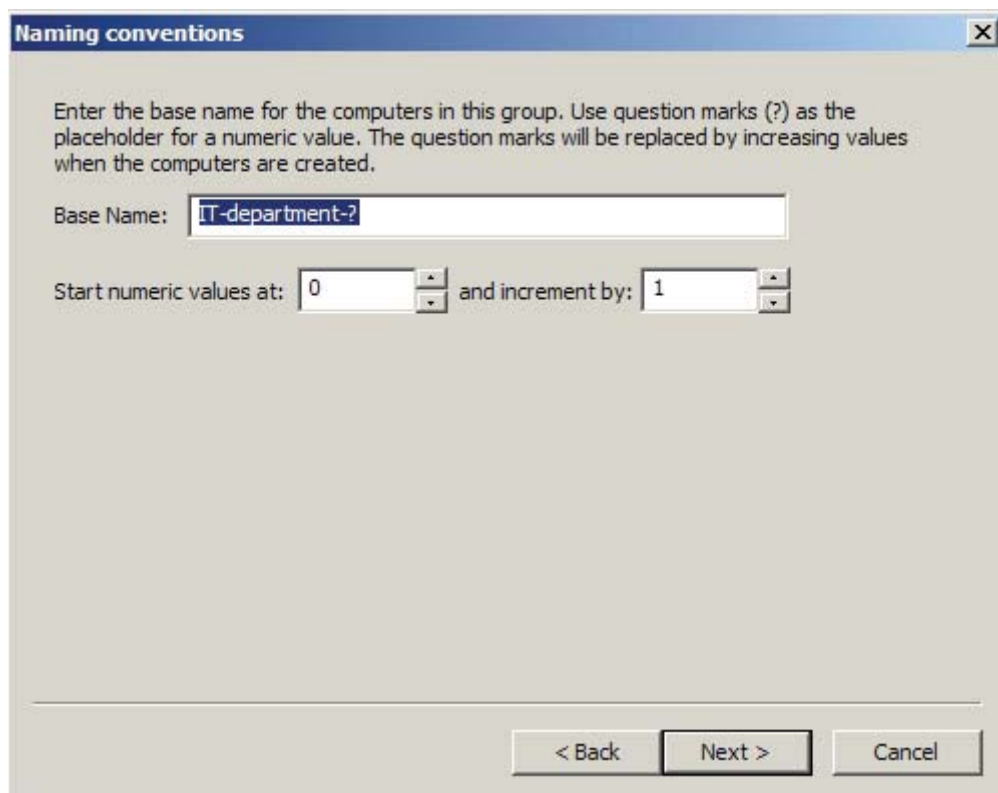
5. Select the snapshot you want linked clone to be created from.



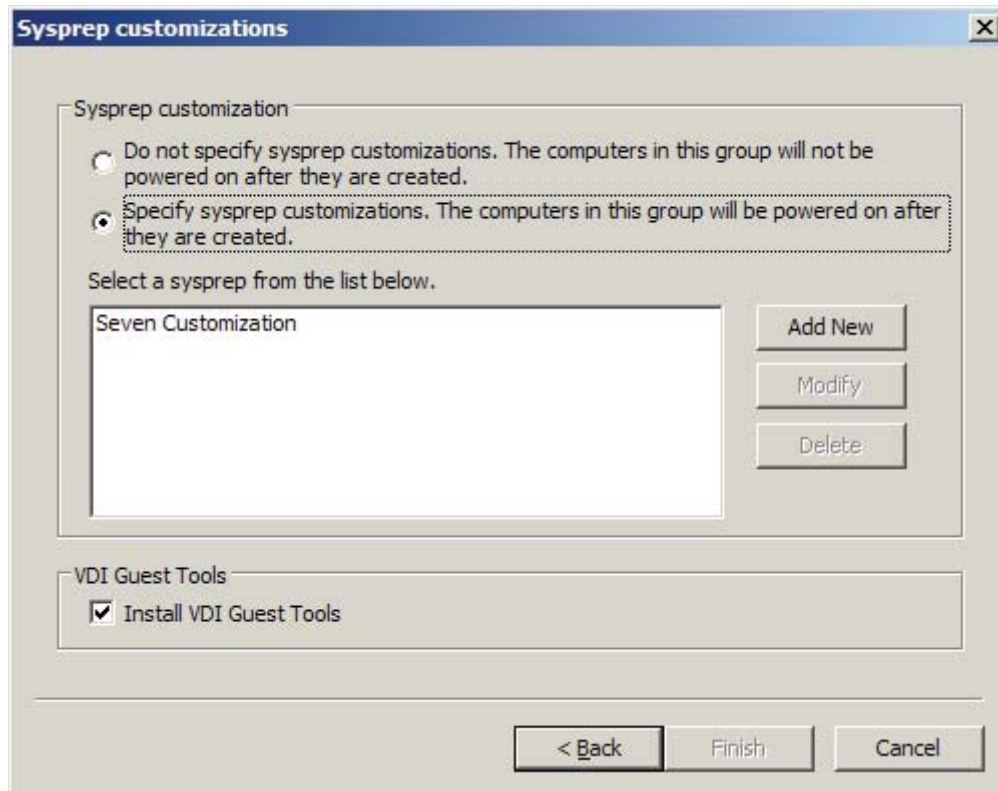
6. Select destination, where VM will be stored after creation. You can select datastore from list of available. Or clone to default destination (where template VM is located). Click *Next*



7. Specify the base name for computers in the group.

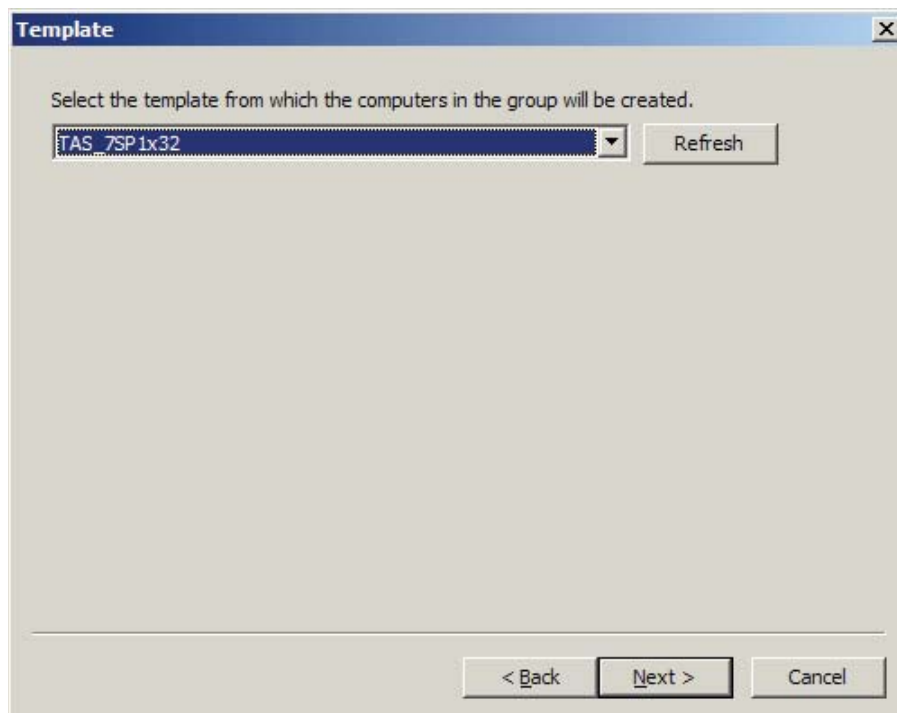


8. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click **Finish**

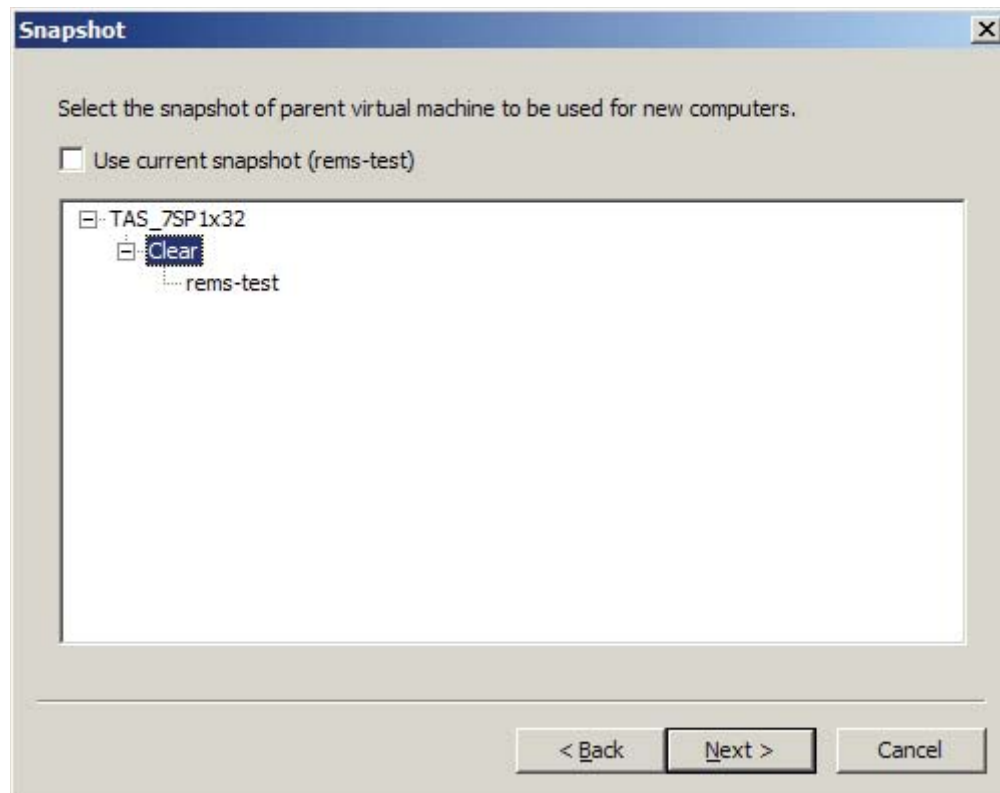


For Standard clone:

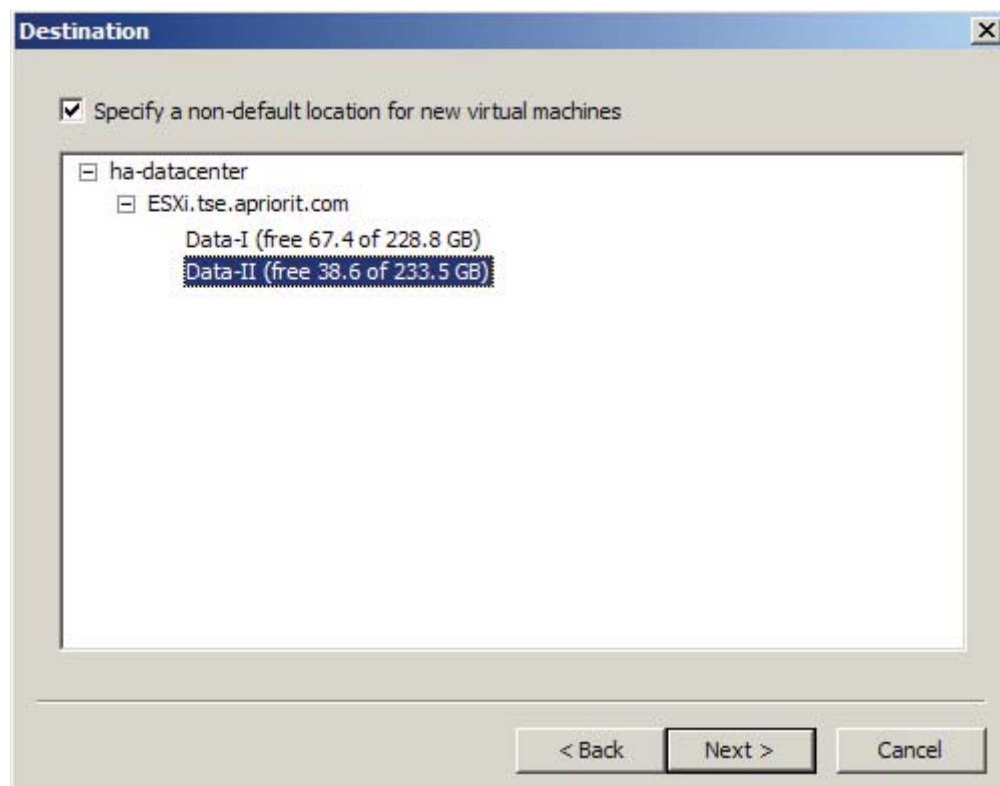
4. Select a *vCenter* virtual machine, which will be used as a template for computers creation. Click *Next*



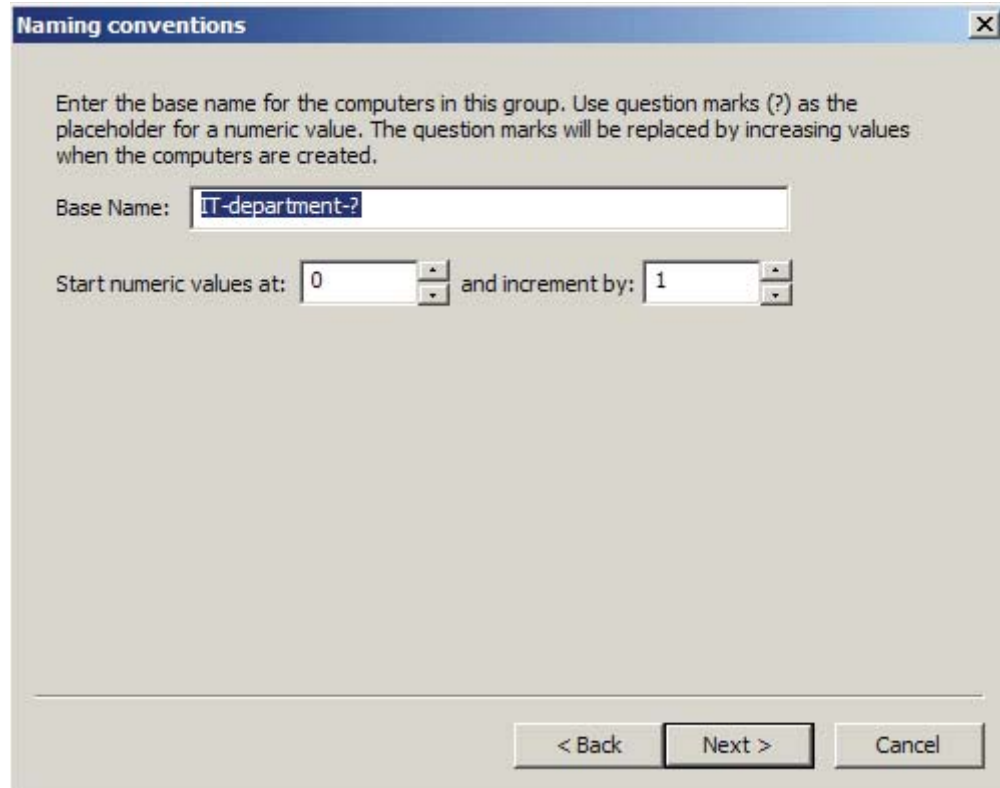
5. Select the snapshot you want linked clone to be created from.



6. Select destination, where VM will be stored after creation. You can select datastore from list of available. Or clone to default destination (where template VM is located). Click *Next*



7. Specify the base name for computers in the group.



Naming conventions

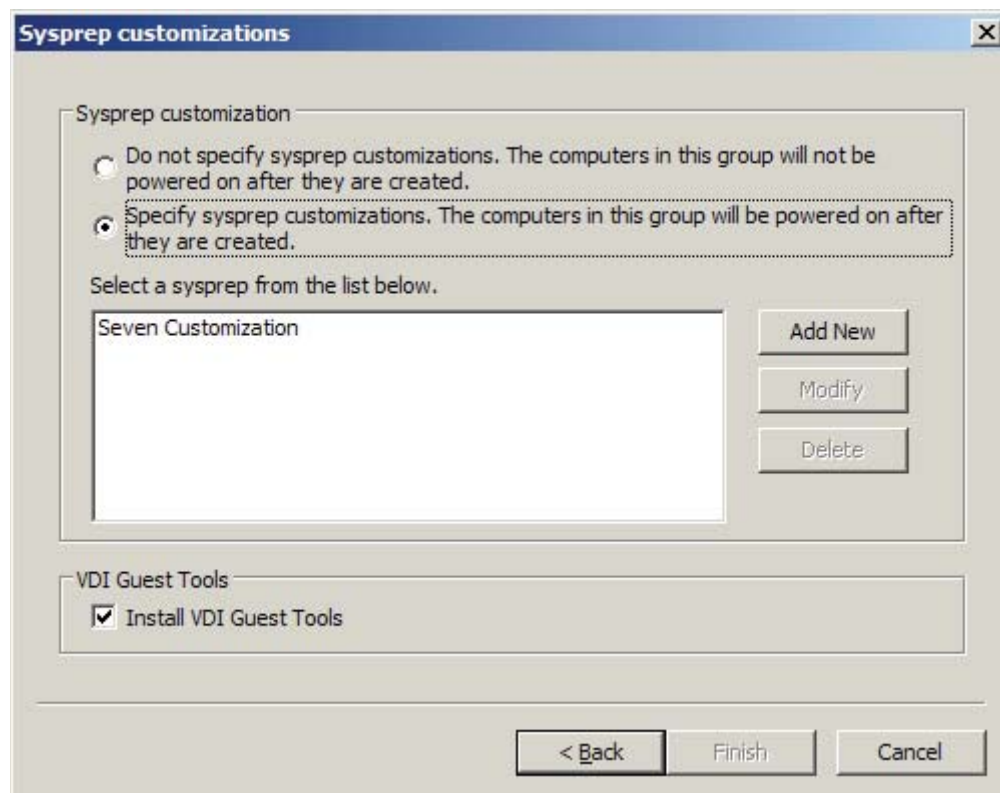
Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.

Base Name:

Start numeric values at: and increment by:

< Back Next > Cancel

8. Specify Sysprep Customization entity. And also choose whether you want to install VDI Guest Tools automatically. Click ***Finish***



Sysprep customizations

Sysprep customization

☐ Do not specify sysprep customizations. The computers in this group will not be powered on after they are created.

☒ Specify sysprep customizations. The computers in this group will be powered on after they are created.

Select a sysprep from the list below.

Seven Customization

Add New Modify Delete

VDI Guest Tools

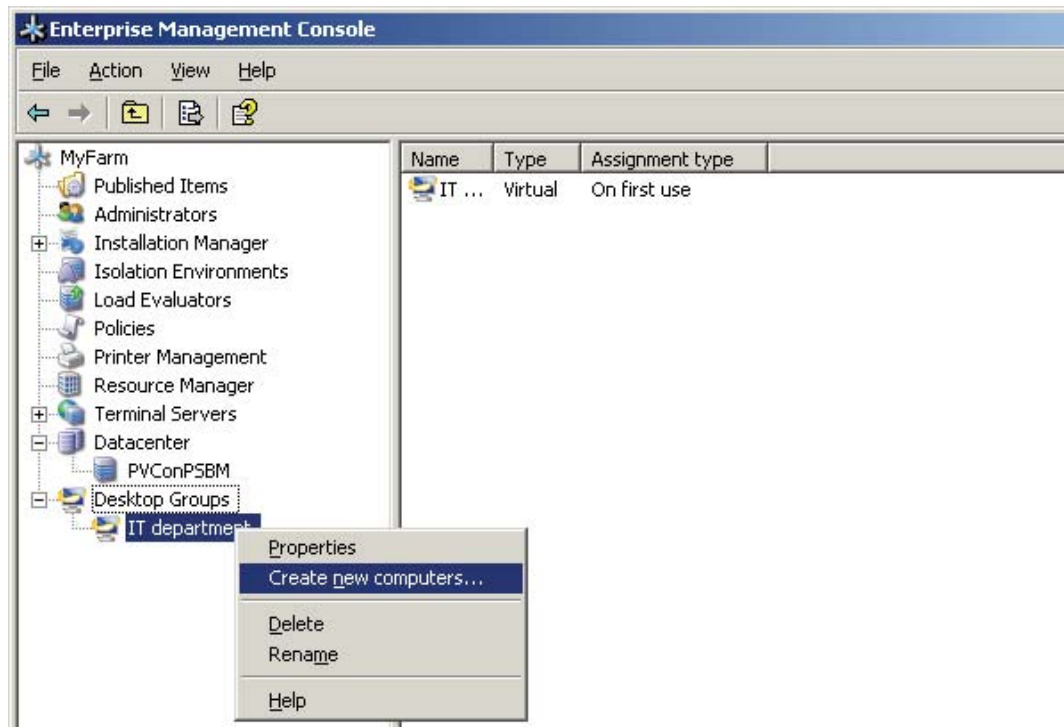
☒ Install VDI Guest Tools

< Back Finish Cancel

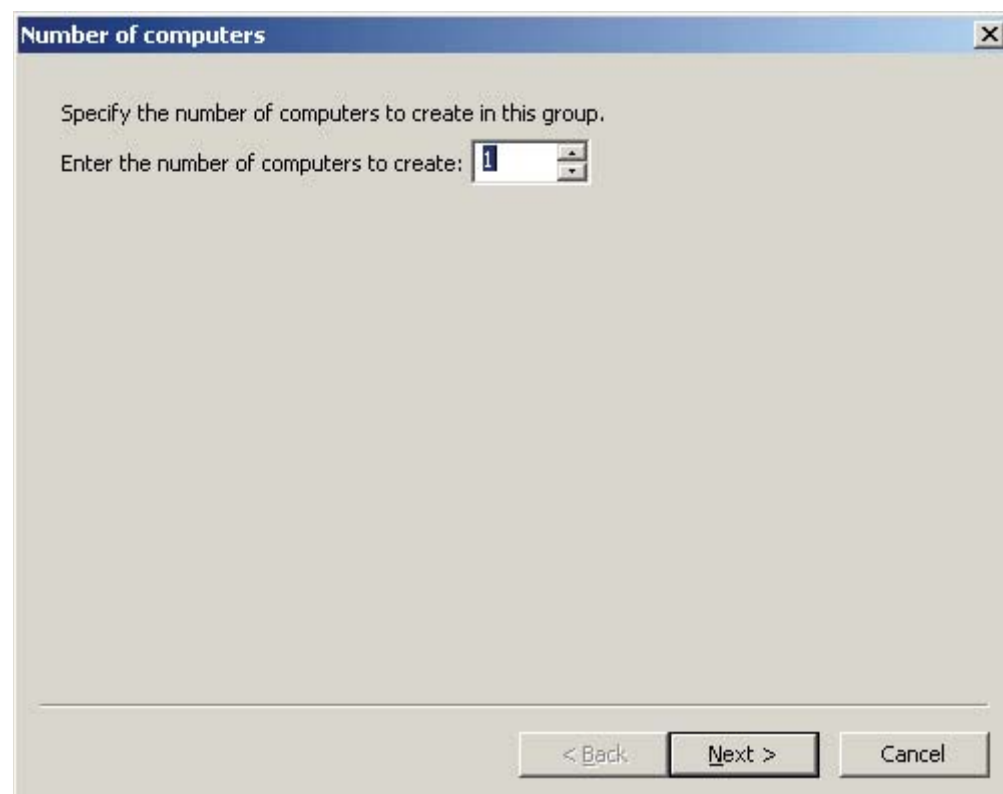
3.14.1.5 Add computer to Parallels Virtuozzo Containers Desktop Group

To create new computers to specific desktop group:

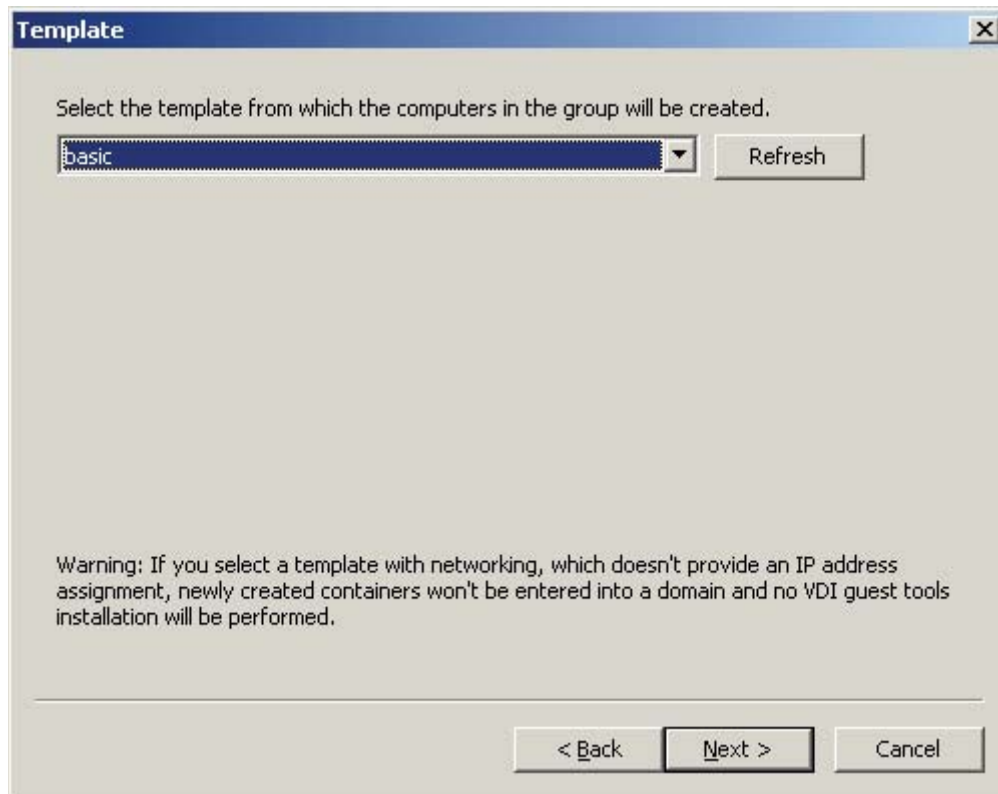
1. Select **Create new computers** item from right-click menu of specific desktop group.



2. Specify the number of computers to create. Click **Next**



3. Select a PVC sample, which will be used as a template for computers creation. Click *Next*



The 'Template' dialog box has a title bar with a close button. The main area contains the instruction 'Select the template from which the computers in the group will be created.' Below this is a dropdown menu with 'basic' selected and a 'Refresh' button to its right. A warning message is displayed below the dropdown: 'Warning: If you select a template with networking, which doesn't provide an IP address assignment, newly created containers won't be entered into a domain and no VDI guest tools installation will be performed.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Template

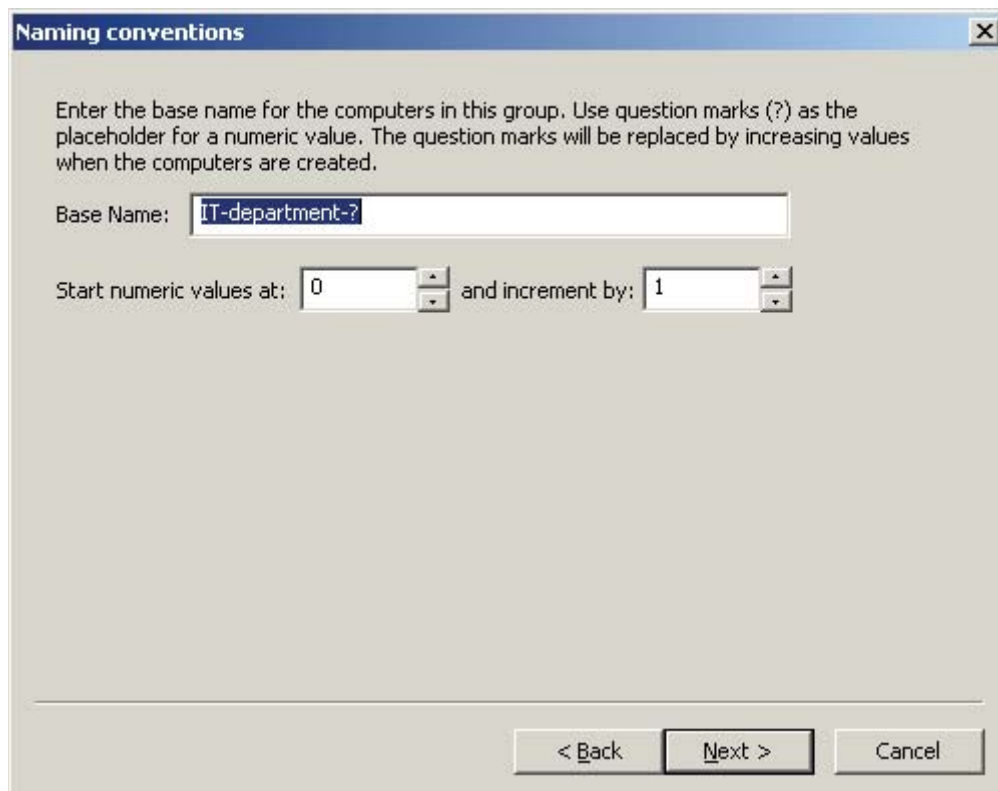
Select the template from which the computers in the group will be created.

basic Refresh

Warning: If you select a template with networking, which doesn't provide an IP address assignment, newly created containers won't be entered into a domain and no VDI guest tools installation will be performed.

< Back Next > Cancel

4. Specify the base name for computers in the group. Click *Next*



The 'Naming conventions' dialog box has a title bar with a close button. The main area contains the instruction 'Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.' Below this is a text field with 'IT-department-?' entered. Underneath are two numeric input fields: 'Start numeric values at:' followed by a field containing '0', and 'and increment by:' followed by a field containing '1'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Naming conventions

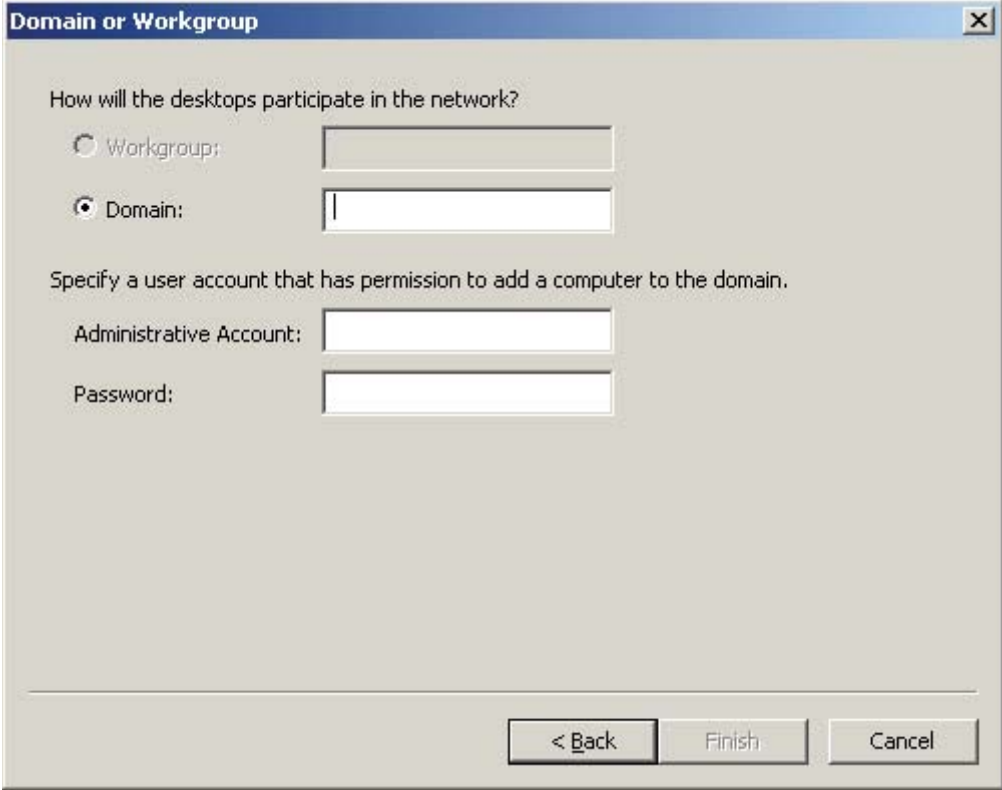
Enter the base name for the computers in this group. Use question marks (?) as the placeholder for a numeric value. The question marks will be replaced by increasing values when the computers are created.

Base Name: IT-department-?

Start numeric values at: 0 and increment by: 1

< Back Next > Cancel

5. Enter the domain information. Click *Finish*



Domain or Workgroup [X]

How will the desktops participate in the network?

☐ Workgroup:

☒ Domain:

Specify a user account that has permission to add a computer to the domain.

Administrative Account:

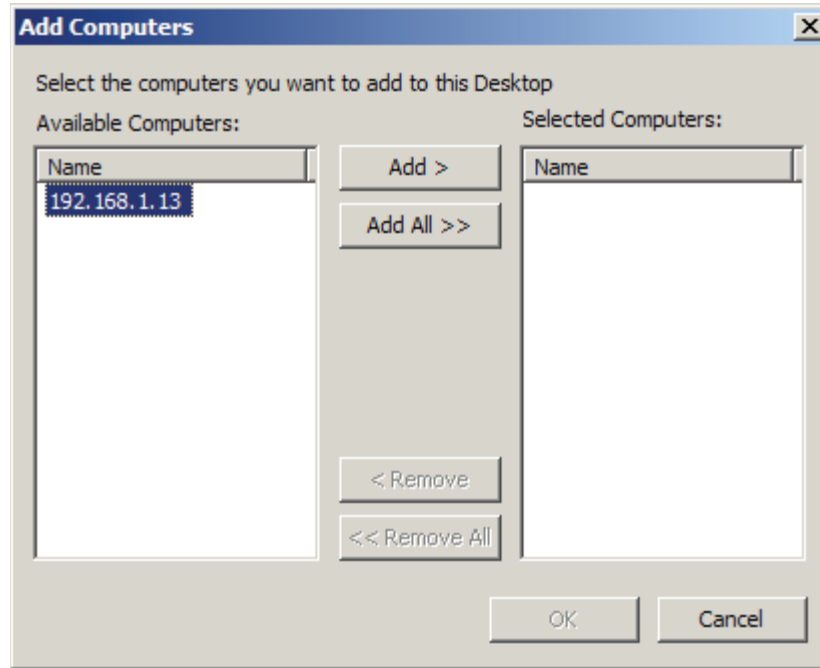
Password:

< Back Finish Cancel

3.14.1.6 Add computer to Other/Physical Desktop Group

To create new computers to specific desktop group:

1. Select **Add computers** item from right-click menu of specific desktop group.
2. Select the computers you want to add to this Desktop Group. Click **OK**

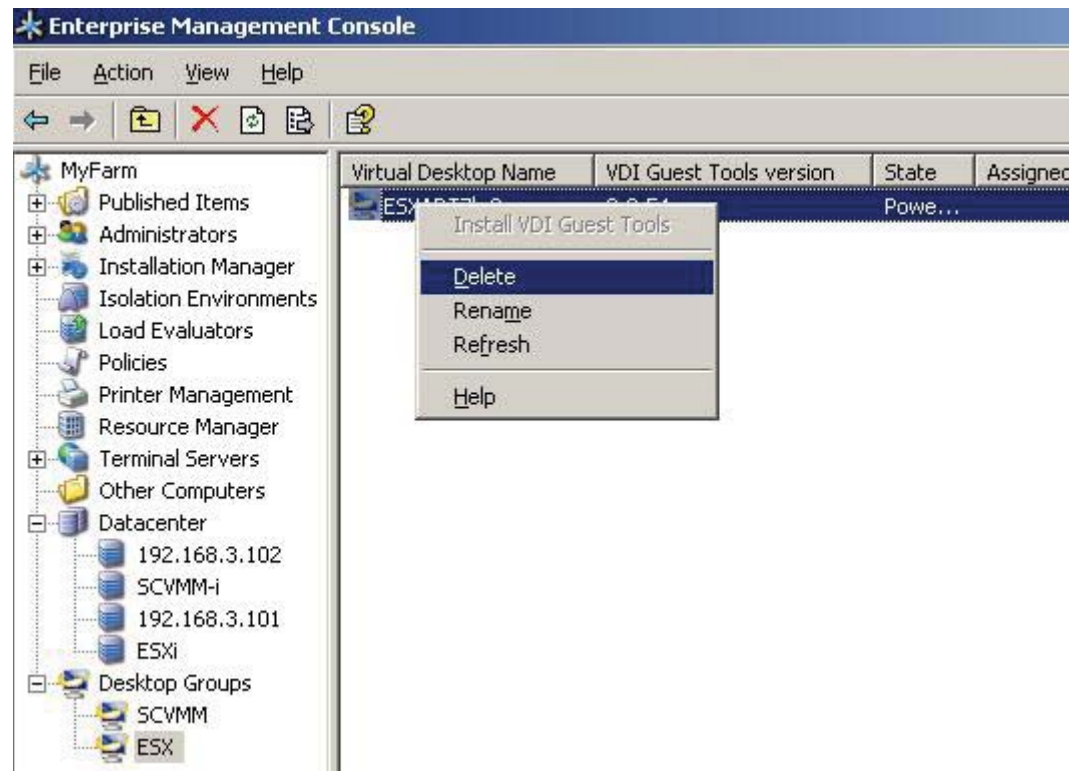


Available Computers list includes computers added to **Other Computers** node, which were not used as Terminal Servers or Datacenters in EMC.

3.14.2 Deleting Computers from Desktop Groups

To Delete Computers from Desktop Group:

1. Select **Delete** item from Created Computers right-click menu. **Confirmation window** appears.



2. Click **Yes** if you sure to delete this VM.



3.15 Installing VDI Guest Tools

Guest Tools – this is extension, which is installed on each virtual and physical machine in a managed desktop group, providing features and management functionality for managed computers.

Guest Tools software allows the following features for remote sessions:

TWAIN scanners redirection;

Two-directional high-quality local audio;

Universal Printing;

USB devices redirection;

Guest Tools can be installed:

manually on virtual and physical machine;

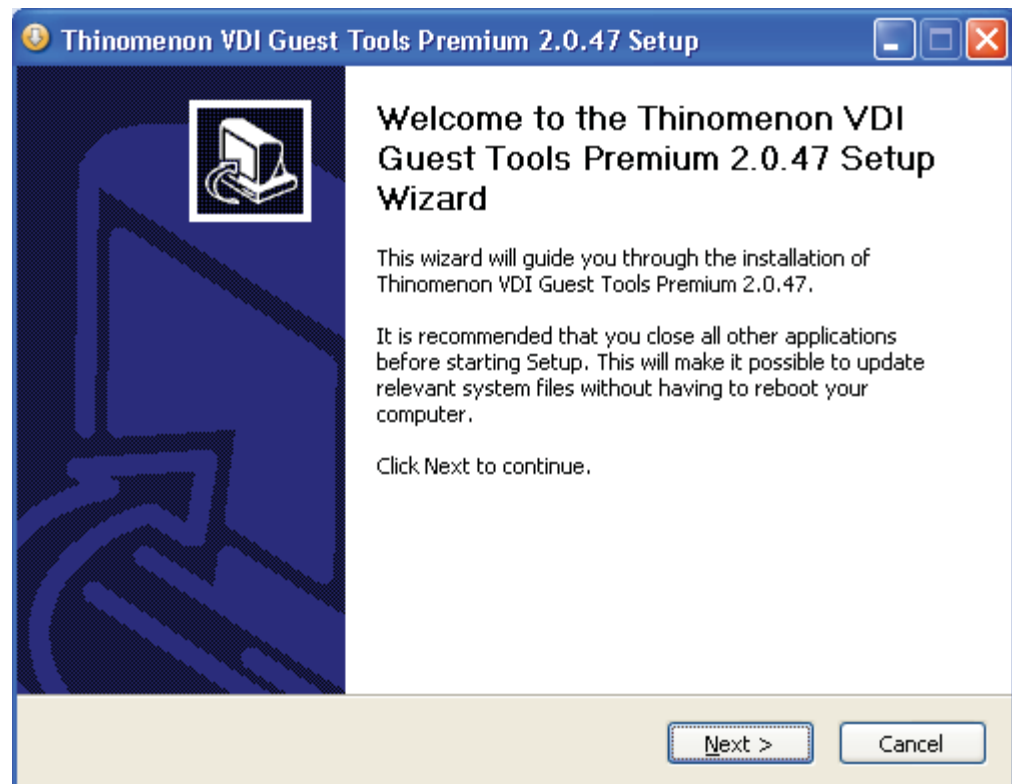
in process of virtual machine creation;

from Management Console to selected virtual machines;

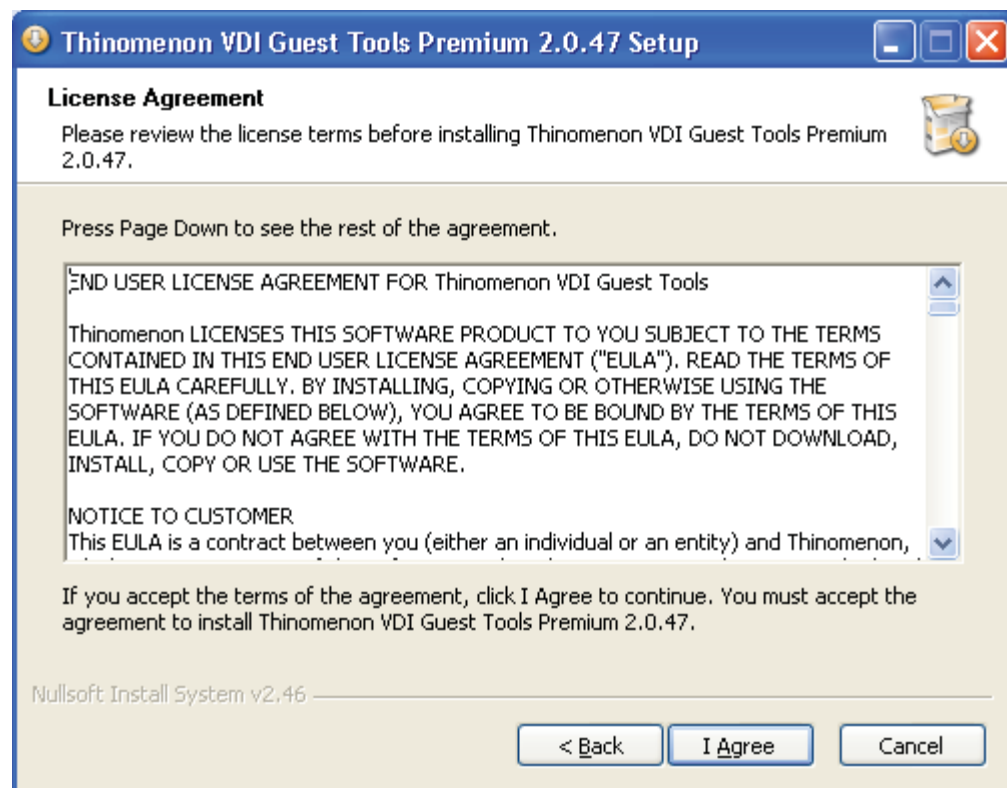
3.15.1 Manual VDI Guest Tools installation

To install VDI Guest Tools manually:

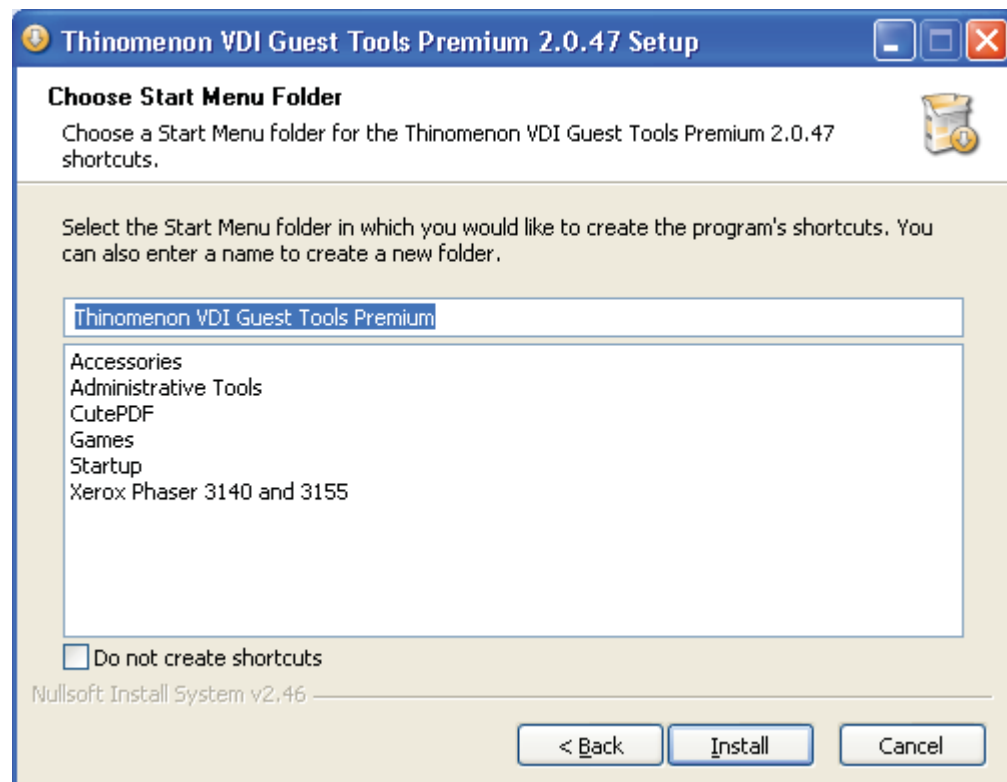
1. Launch the installer



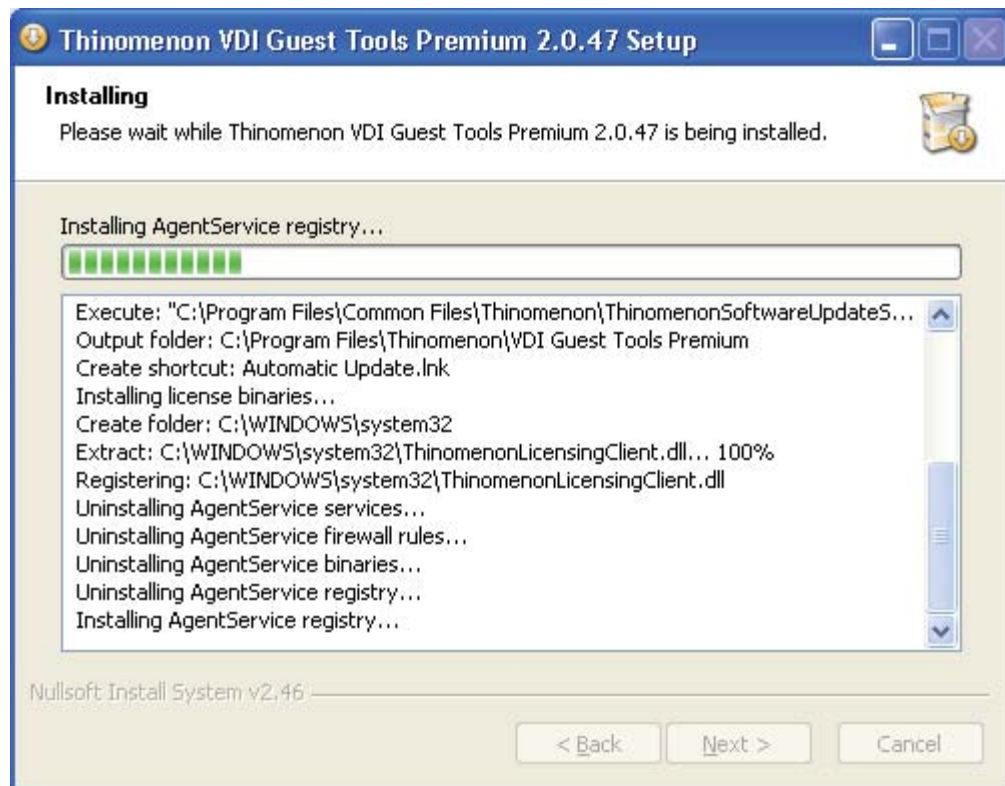
2. Read and accept the license:



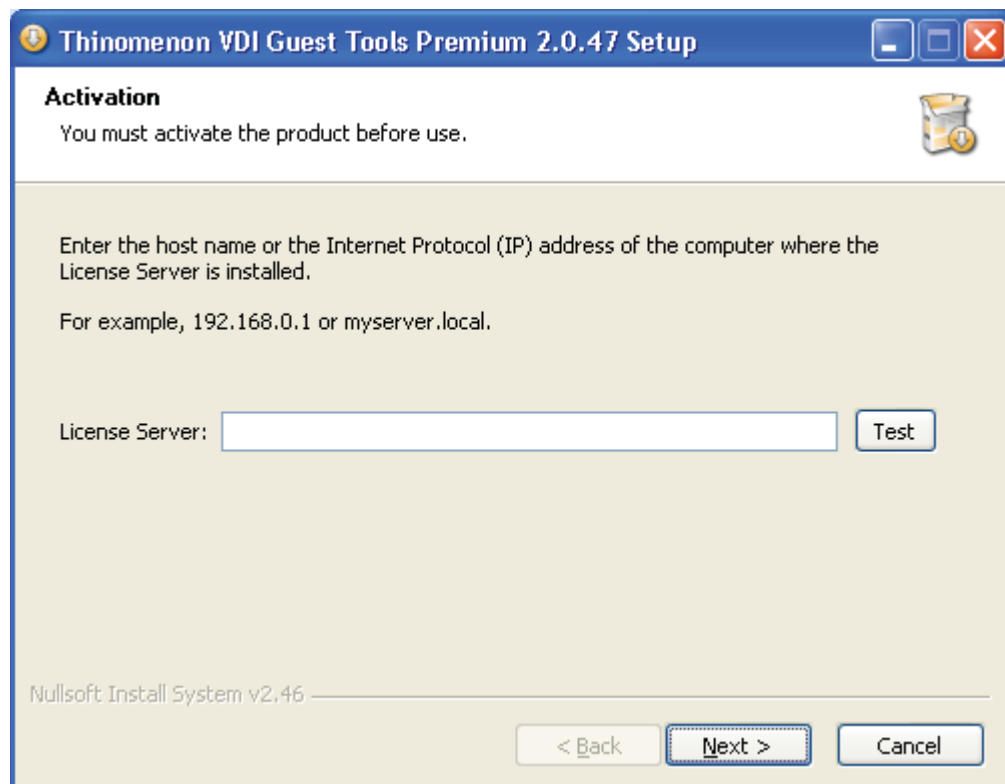
3. Choose Start menu folder:



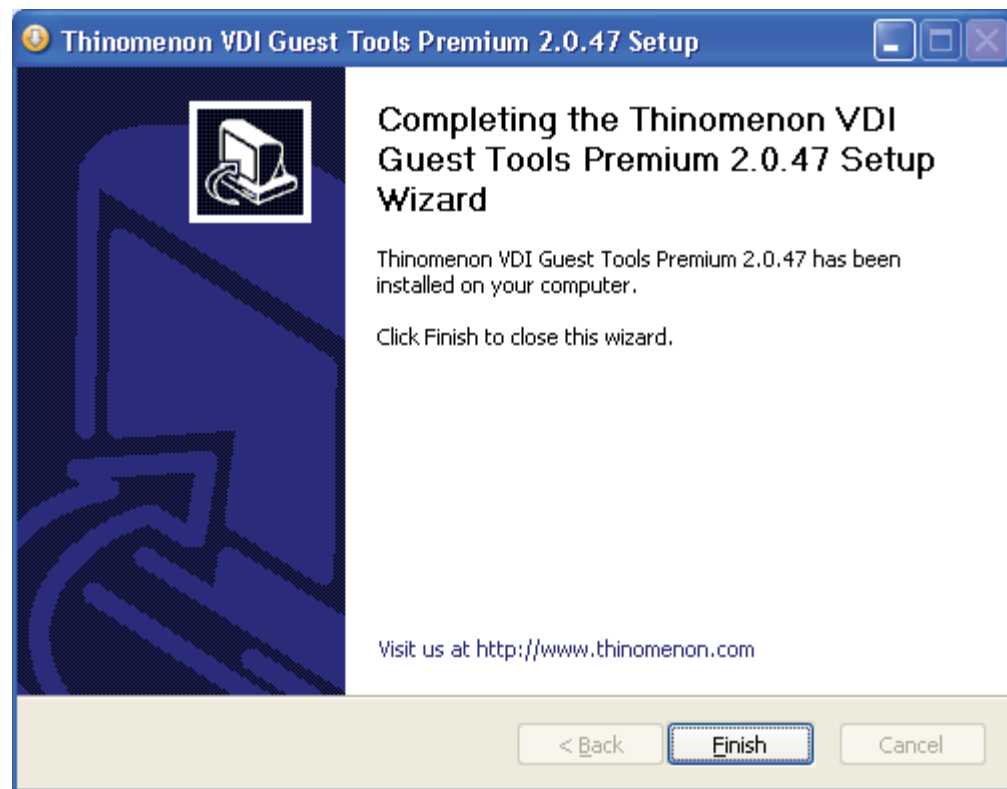
4. Installation is in progress:



5. Specify the valid License Server:



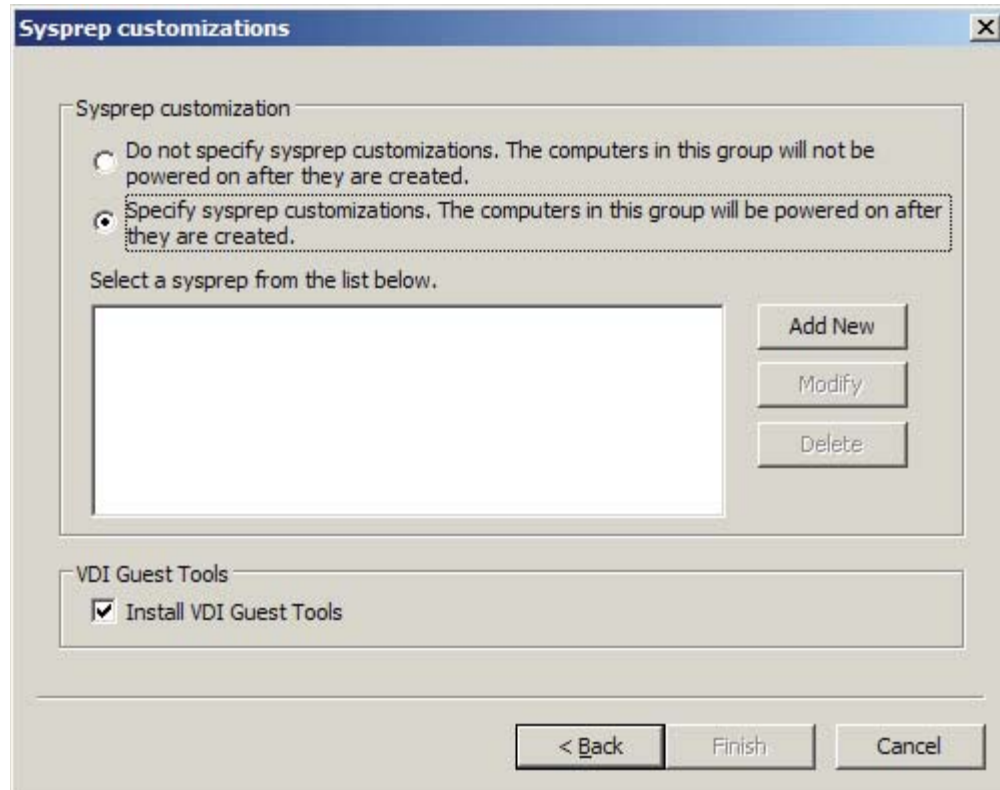
6. We have successfully installed VDI Guest Tools:



3.15.2 Guest Tools installation in process of virtual machine creation

To install Guest Tools in process of virtual machine creation:

1. Check **Install VDI Guest Tools** option on **Sysprep customizations** window in **Create New computers** wizard as shown below:

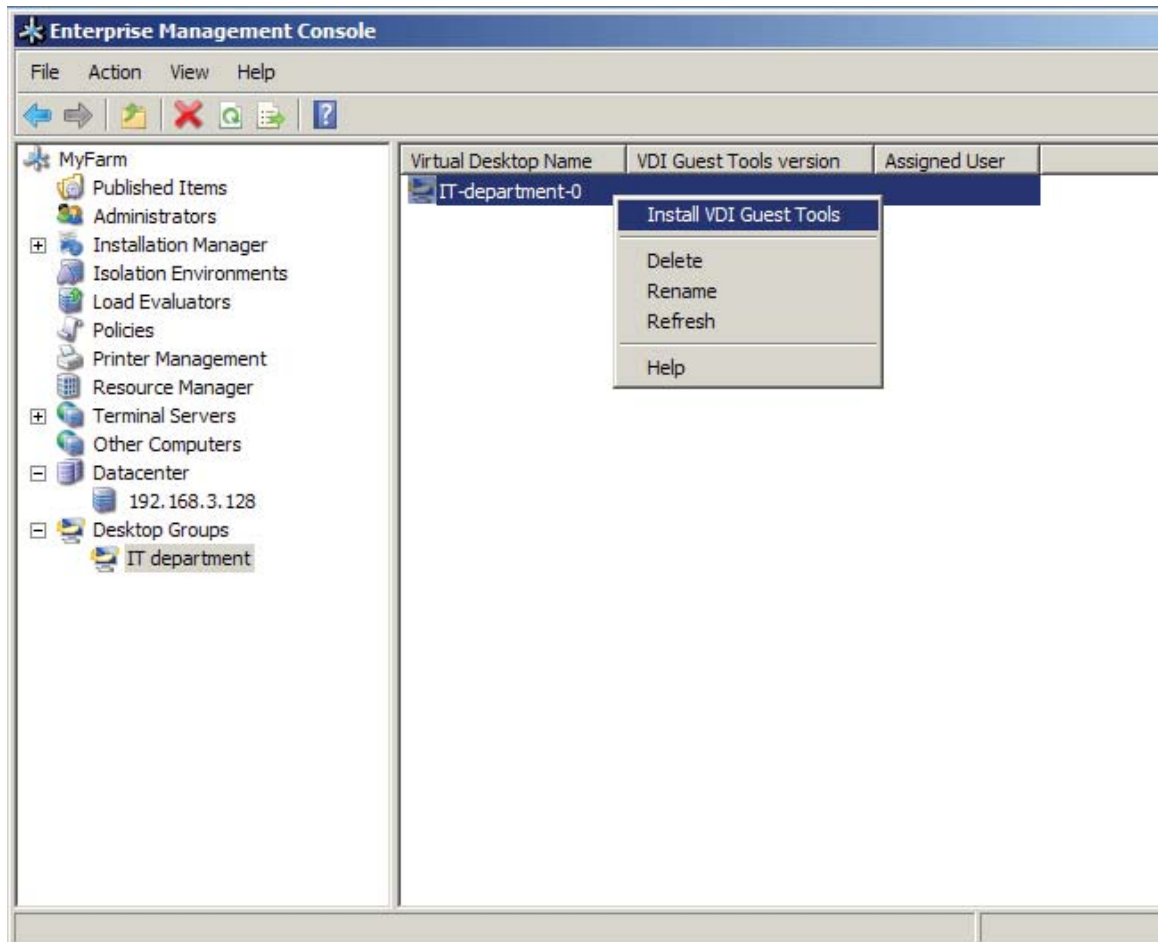


2. Guest Tools will be installed automatically after virtual machine creation process is finished.

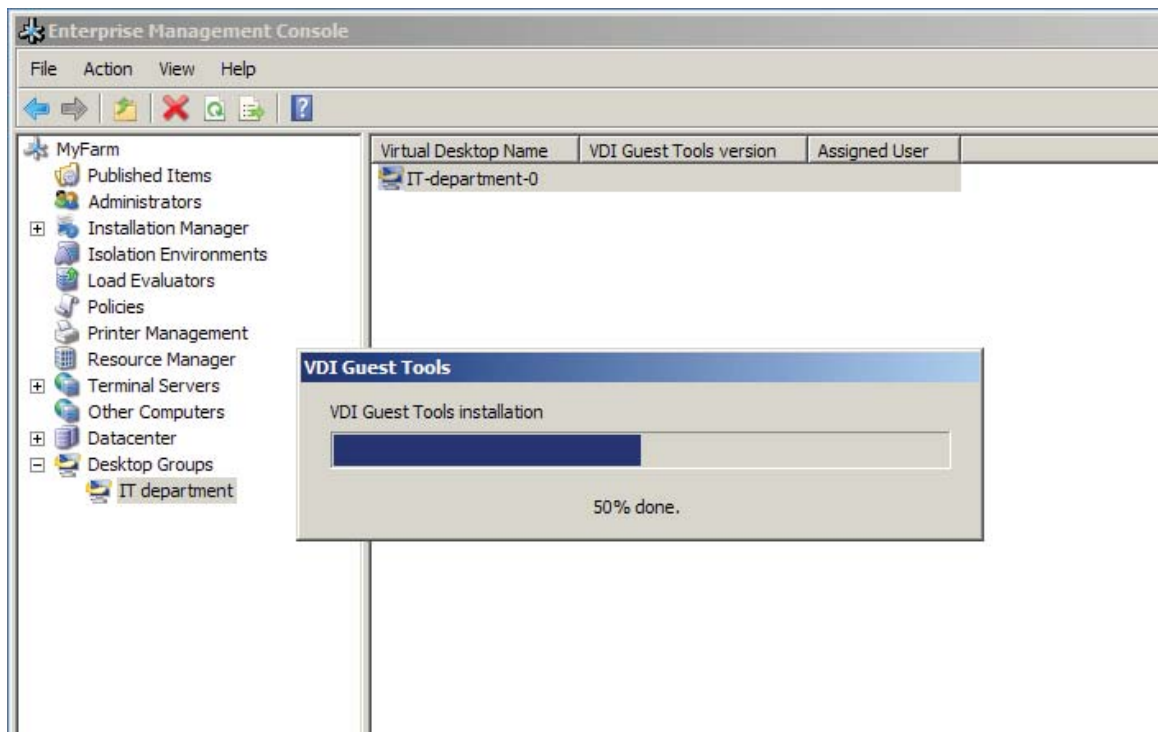
3.15.3 Guest Tools Installation from Management Console

To Install VDI Guest Tools from Management Console:

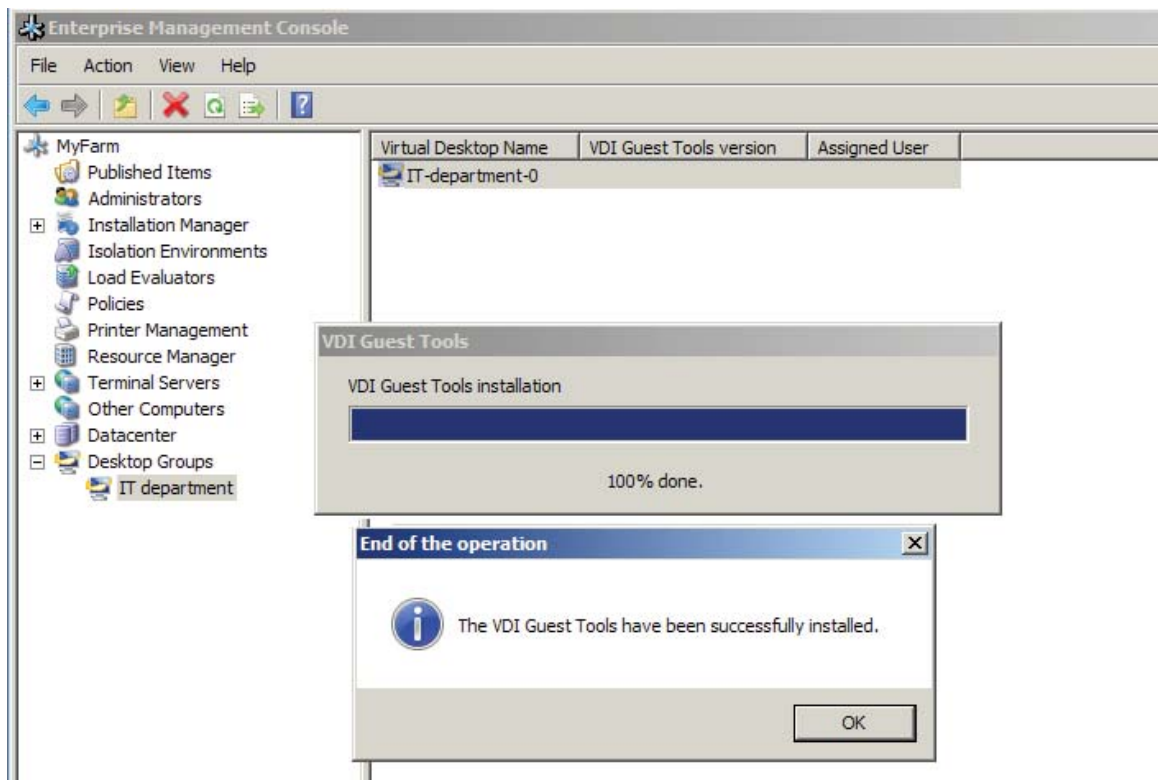
1. Select ***Install VDI Guest Tools*** item from right-click menu of *virtual machine*.



2. VDI Guest Tools installation is in progress:



3. After Guest Tools installation is finished, appropriate message appears:



3.16 Managing Sysprep Customization

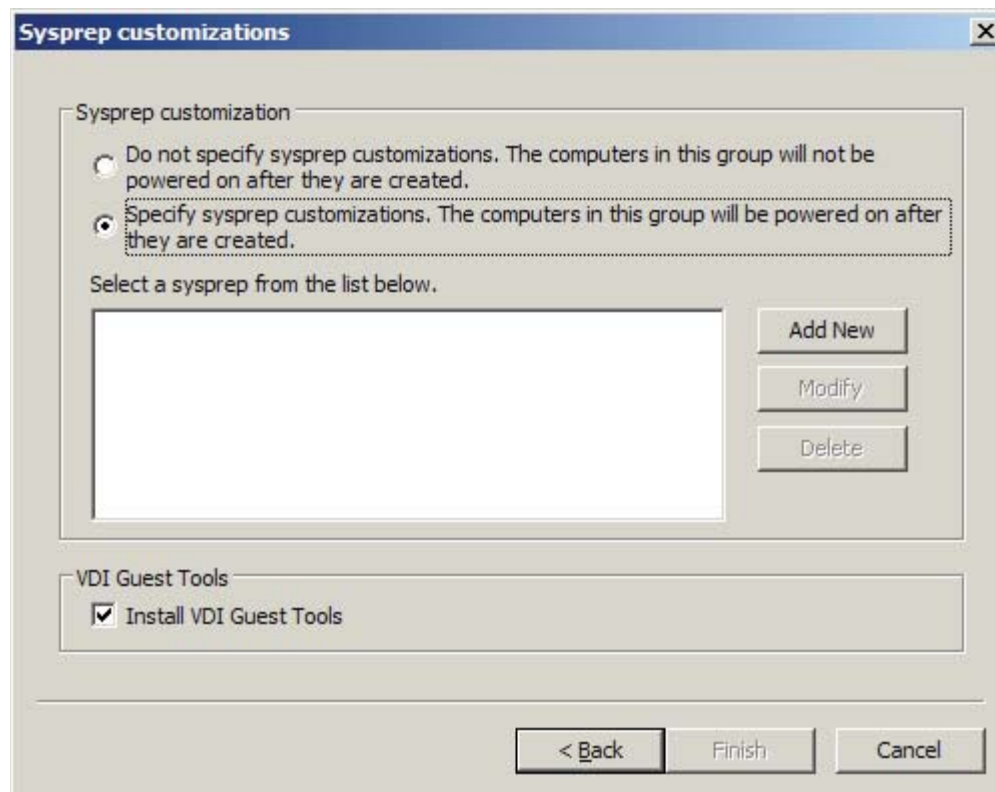
Preparation of just created computers for the 1-st use (joining the domain, setting time zone etc) is performed with help of Microsoft's System Preparation Utility (Sysprep).

To apply Sysprep customization after cloning process you need to create one or more Sysprep entities. It depends on operating systems, which are planned to be used.

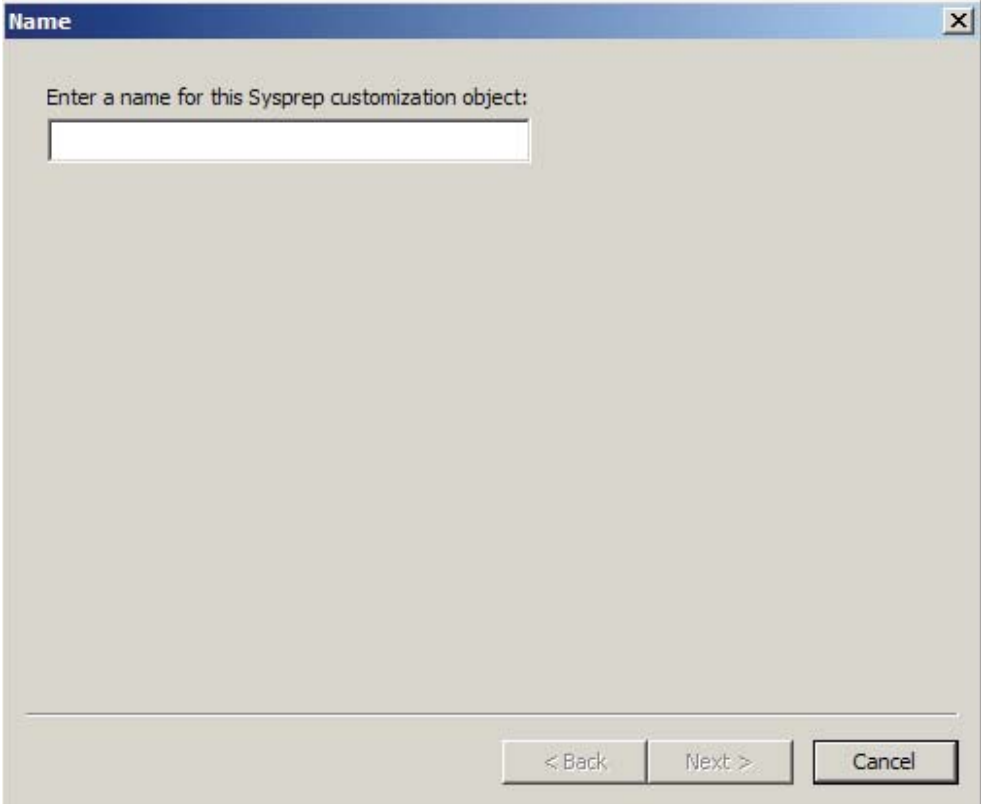
3.16.1 Adding New Sysprep Customization

To Add new Sysprep entity:

1. Click **Add New** on **Sysprep customizations** window during virtual machine creation:

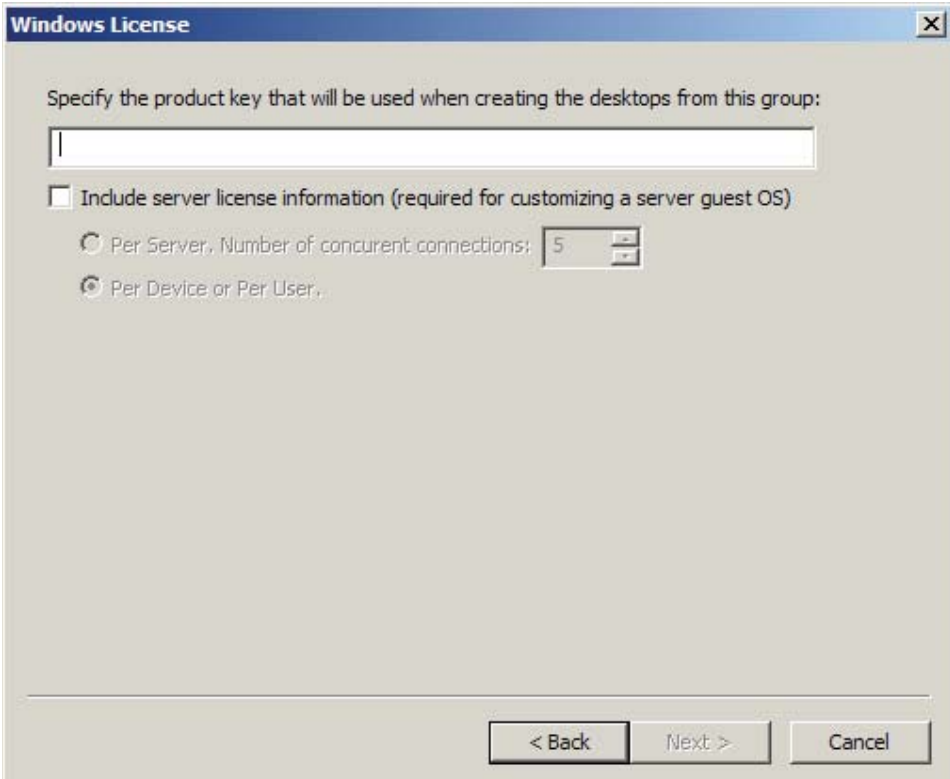


2. Enter friendly name for Sysprep entity:



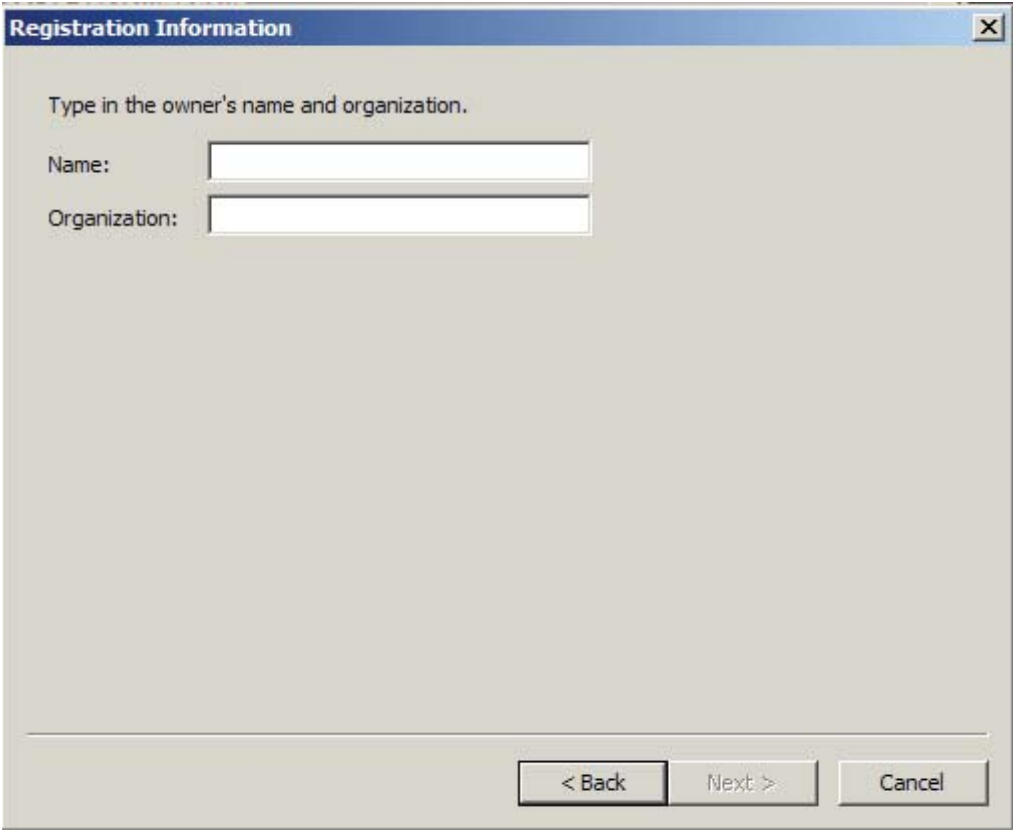
A dialog box titled "Name" with a close button (X) in the top right corner. The main area contains the text "Enter a name for this Sysprep customization object:" followed by a single-line text input field. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

3. Specify Windows product key:



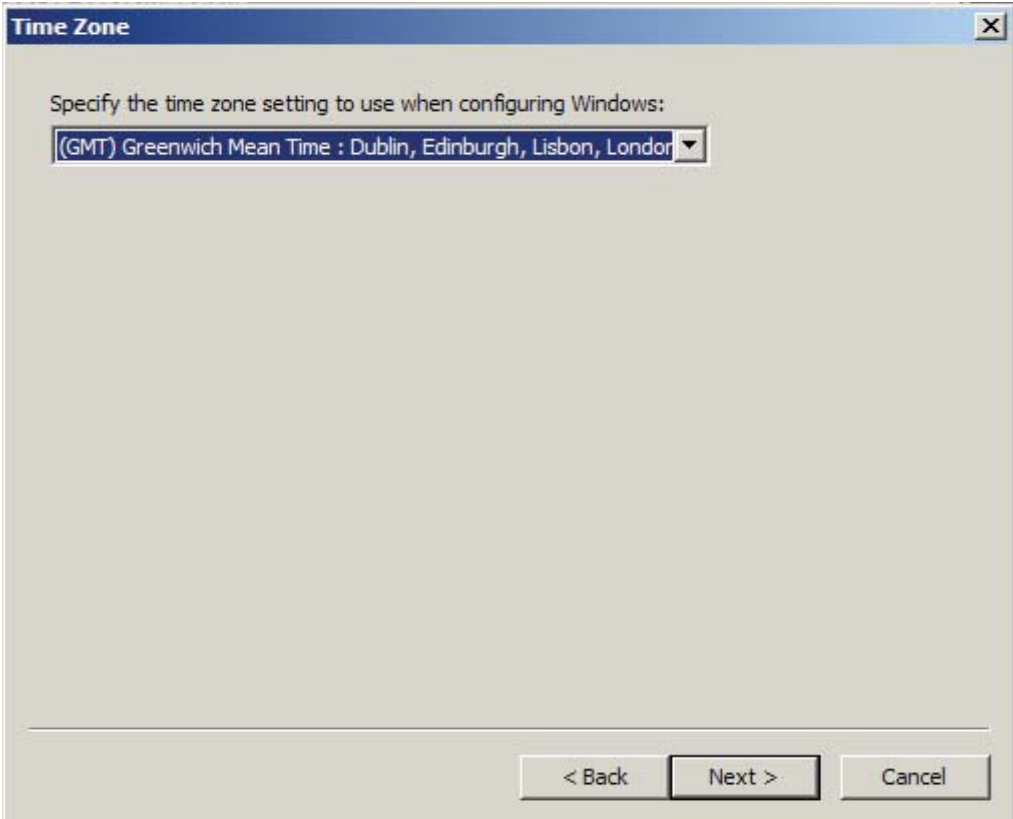
A dialog box titled "Windows License" with a close button (X) in the top right corner. The main area contains the text "Specify the product key that will be used when creating the desktops from this group:" followed by a single-line text input field. Below this is a checkbox labeled "Include server license information (required for customizing a server guest OS)". If checked, there are two radio button options: "Per Server, Number of concurrent connections:" with a numeric input field set to "5", and "Per Device or Per User,". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter owner's information:



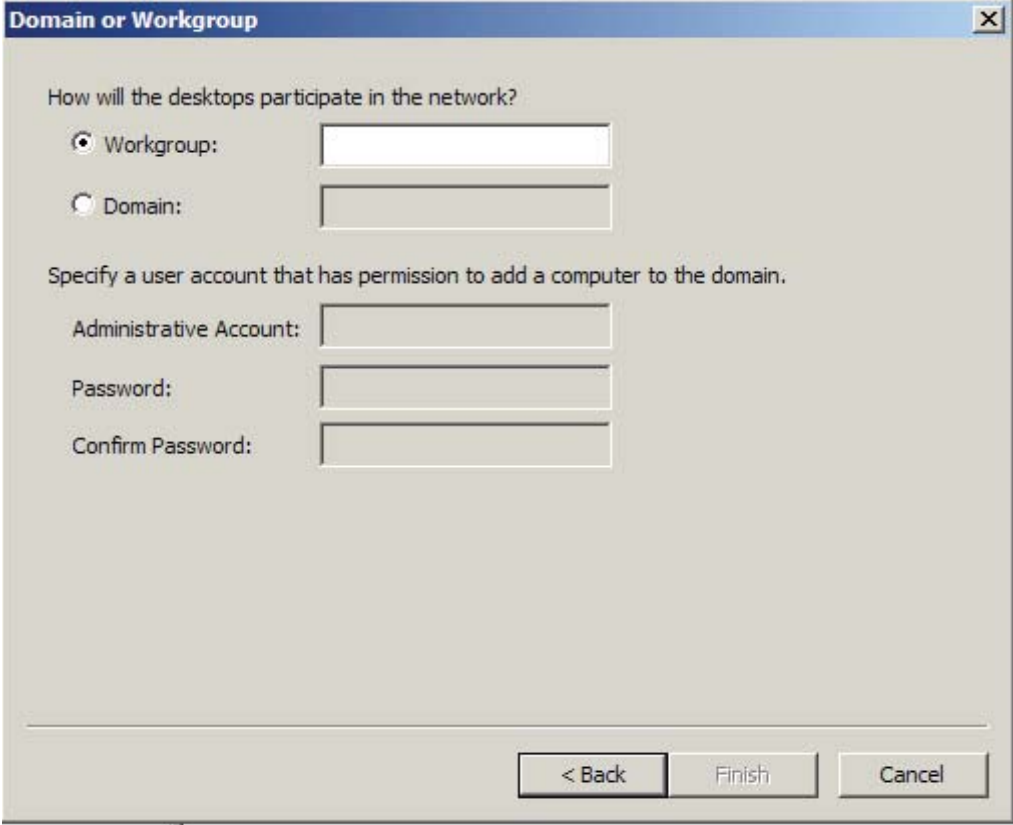
The 'Registration Information' dialog box has a blue title bar with the text 'Registration Information' and a close button (X). The main area is light gray and contains the instruction 'Type in the owner's name and organization.' Below this are two text input fields: 'Name:' and 'Organization:'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Specify your time zone:



The 'Time Zone' dialog box has a blue title bar with the text 'Time Zone' and a close button (X). The main area is light gray and contains the instruction 'Specify the time zone setting to use when configuring Windows:'. Below this is a dropdown menu showing '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Join Computer to Domain or Workgroup. To join computer to Domain you must specify credentials of domain user who has the permission to add computers to domain:



Domain or Workgroup

How will the desktops participate in the network?

☒ Workgroup:

☐ Domain:

Specify a user account that has permission to add a computer to the domain.

Administrative Account:

Password:

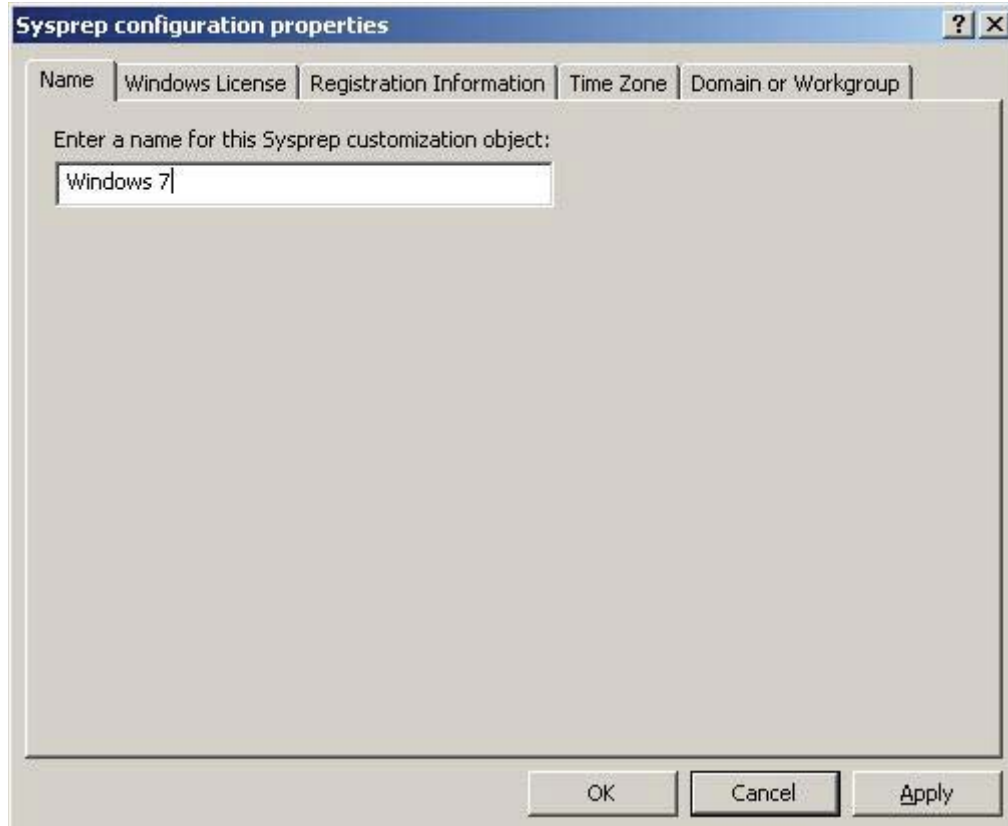
Confirm Password:

< Back Finish Cancel

3.16.2 Modifying Sysprep Customization

To Modify Sysprep Customization:

1. Select Sysprep entity you want to modify On *Sysprep customizations* window during virtual machine creation
2. Click **Modify**. A Sysprep configuration properties appears.



3. After you make changes click **OK**.

3.16.3 Deleting Sysprep Customization

To Delete Sysprep Customization:

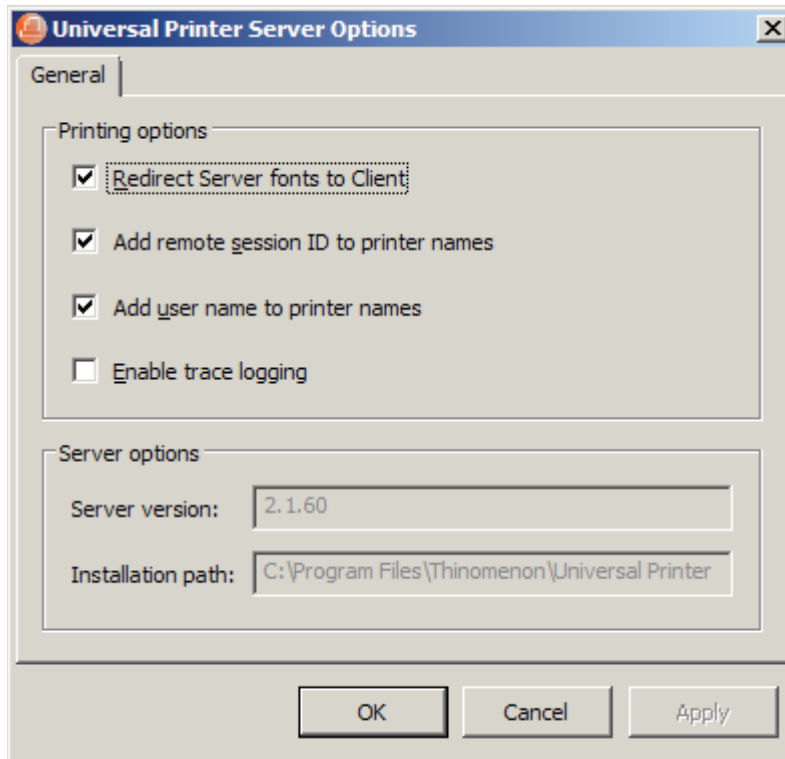
1. Select Sysprep entity you want to delete On *Sysprep customizations* window during virtual machine creation
2. Click **Delete**.

3.17 Managing Universal Printer Server options

Universal Printer comes as part of Member Server, enhancing Remote Desktop printing with driver-free technology that eliminates the need for printer driver administration in terminal services environments.

To use Universal Printing in remote sessions turn on the appropriate option in Access Client (Universal Printing for Web Client is turned on by default).

Also there are Universal Printer options, which are accessible from Control panel of host with Member Server installed:



3.17.1 Enable Server fonts redirection to Client

Redirect Server fonts to Client – turn on/off font redirection from server to client when printing. Changes according to this option are applied with next printing.

To enable server fonts redirection to Client:

1. Open *Universal Printer Server Options* from *Control Panel*
2. Check Redirect Server fonts to Client option. Click **OK**

3.17.2 Enable adding remote session ID to printer names

Add remote session ID to printer names – adding IDs of remote sessions to printer names, it helps to avoid possible conflicts with printer names in session. Changes according to this option are applied with launching of new remote session with Universal Printer.

To enable adding remote session ID to printer names:

1. Open ***Universal Printer Server Options*** from ***Control Panel***
2. Check Add remote session ID to printer names option. Click ***OK***

3.17.3 Enable adding user name to printer names

Add user name to printer name – adding username to printer name, it serves for visibility so user with administrative rights can see user users' redirected printers. Changes according to this option are applied with launching of new remote session with Universal Printer.

To enable adding user name to printer names:

1. Open ***Universal Printer Server Options*** from ***Control Panel***
2. Check Add user name to printer names option. Click ***OK***

3.17.4 Enable trace logging

Enable trace logging – turn on/off logging for server part of Universal Printer. Changes according to this option are applied immediately. Log will be saved to ***INSTALLDIR\UPrinter.log***, where ***INSTALLDIR*** is a directory where Member Server was installed.

To enable trace logging:

1. Open ***Universal Printer Server Options*** from ***Control Panel***
2. Check Enable trace logging option. Click ***OK***

4 Working with Client Software

End-users can connect to full-featured desktops and applications, published in a Thinomenon infrastructure, with help of Thinomenon Client software.

There are two available interfaces: Web Client and Access Client.

4.1 Using Web Client

4.1.1 Overview

Access Suite Web Client allows users to access published resources, including applications, documents and full desktops using a Java-enabled web browser.

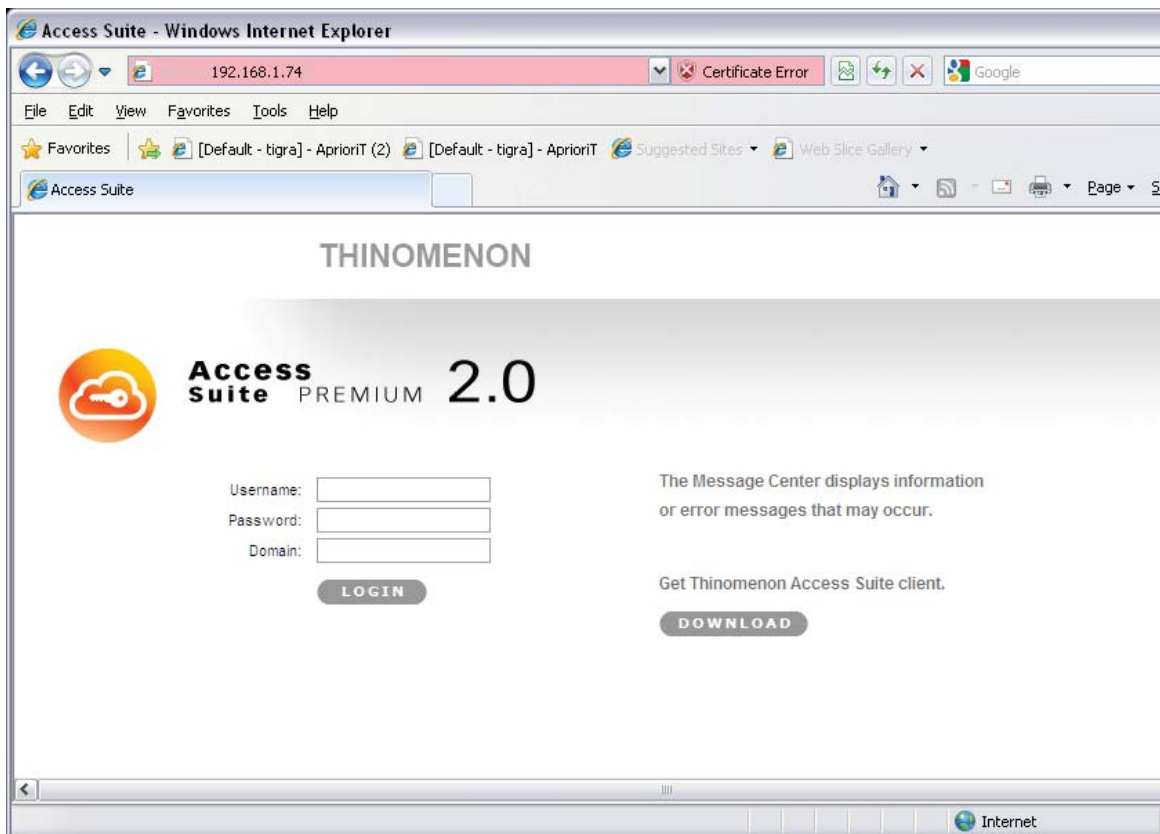
Web Client can be used for access from Windows and Mac OS X.

Web Client will work from a web browser with Java Runtime Environment version 4 or higher installed.

4.1.2 Usage

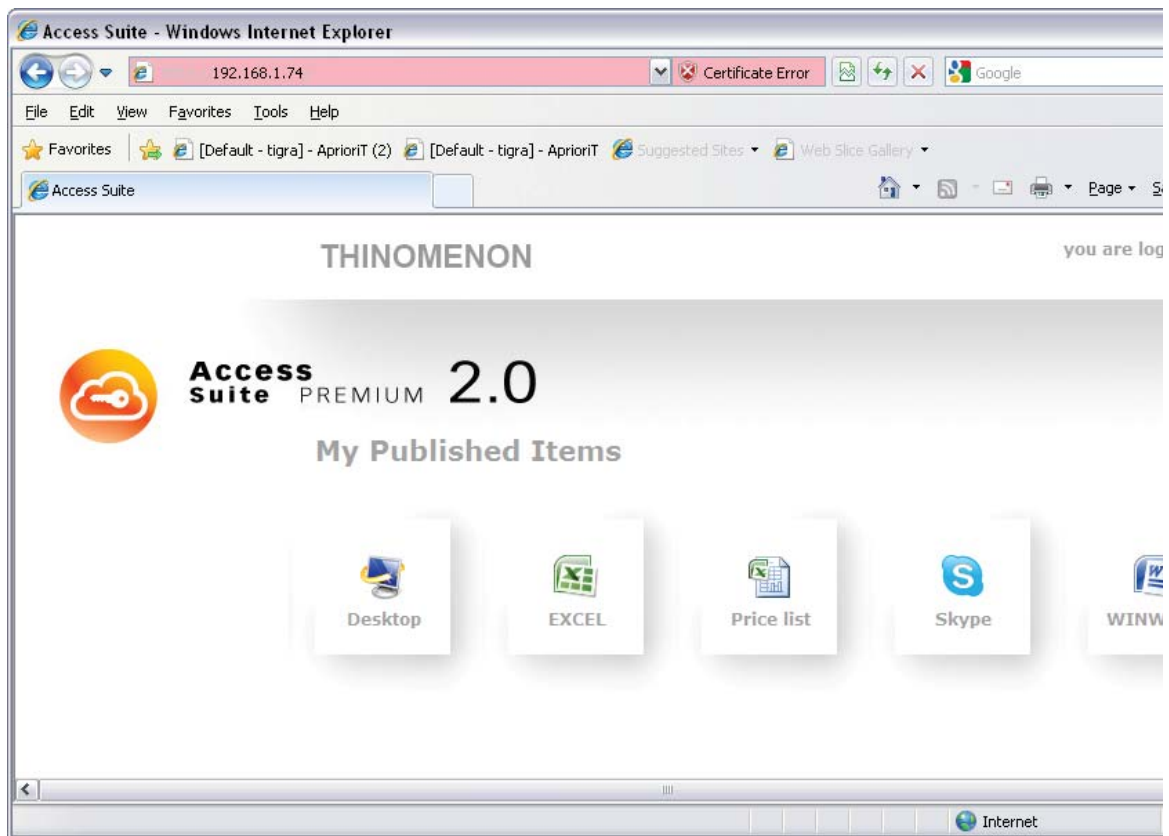
To use Web Client:

1. Launch your web browser and point it to the Web portal:



2. Specify Credentials. Click **Login**. Available published items will be listed in web browser.

3. Click the specific item to launch it.

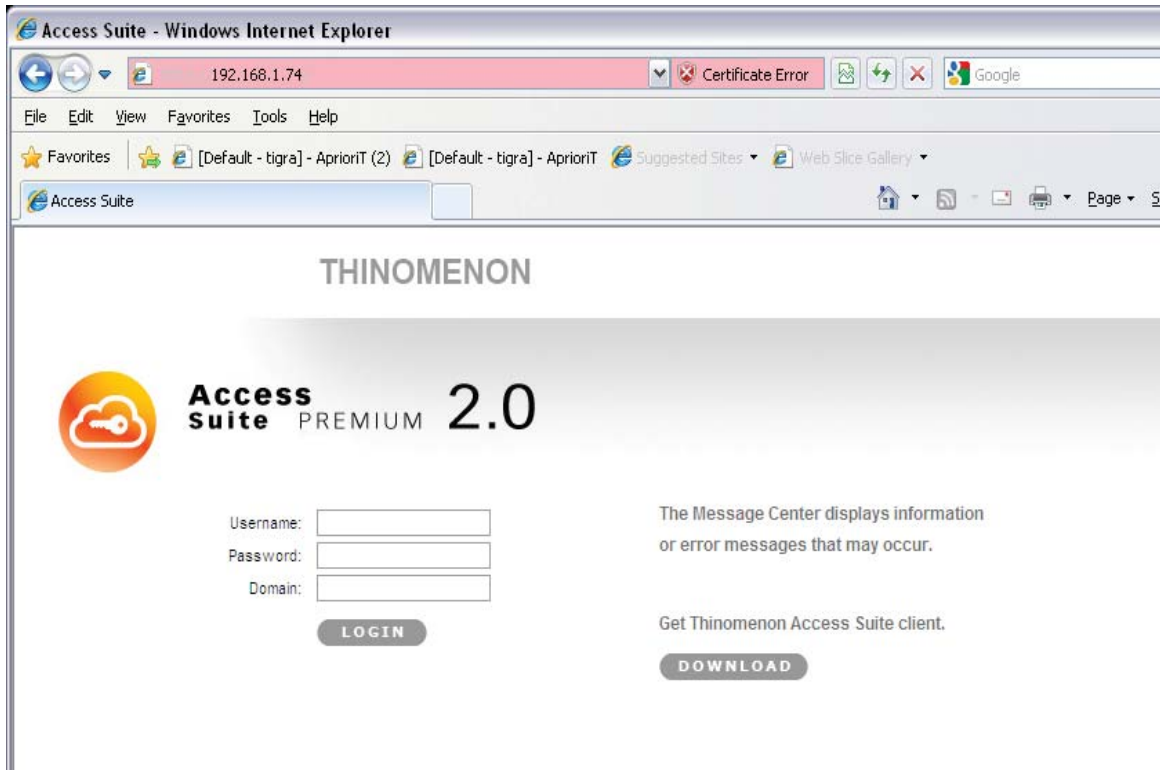


4.2 Using Thinomenon Access Client

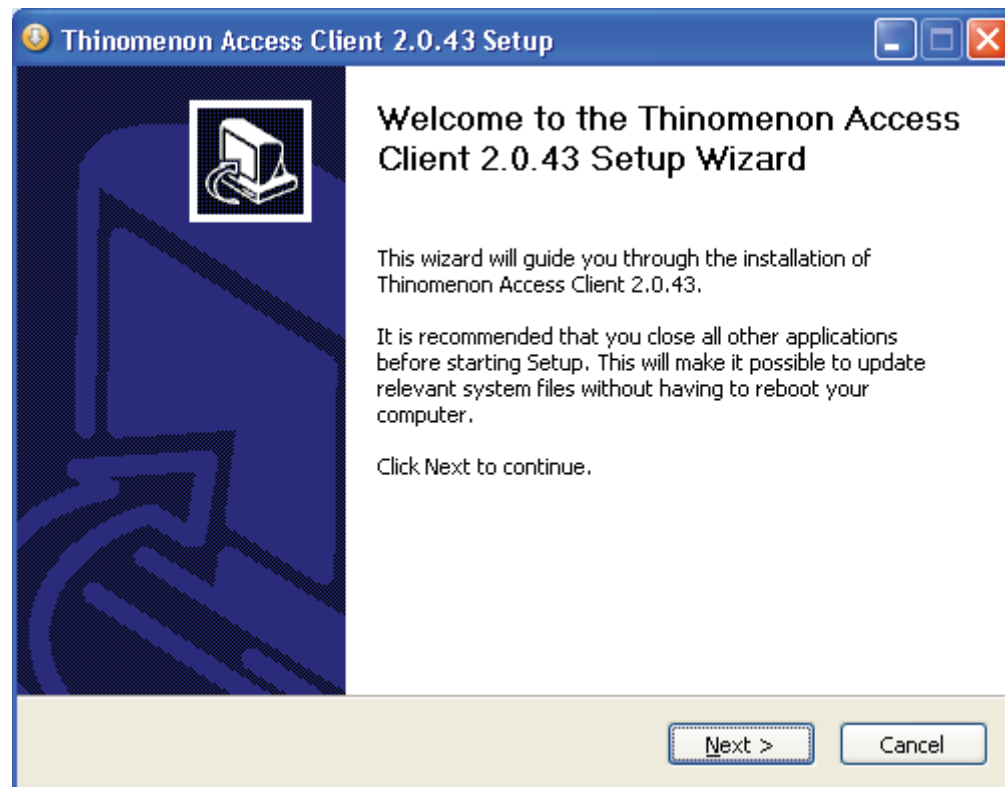
4.2.1 Installing Thinomenon Access Client

Thinomenon Access Suite Client installer can be downloaded from Web Client.

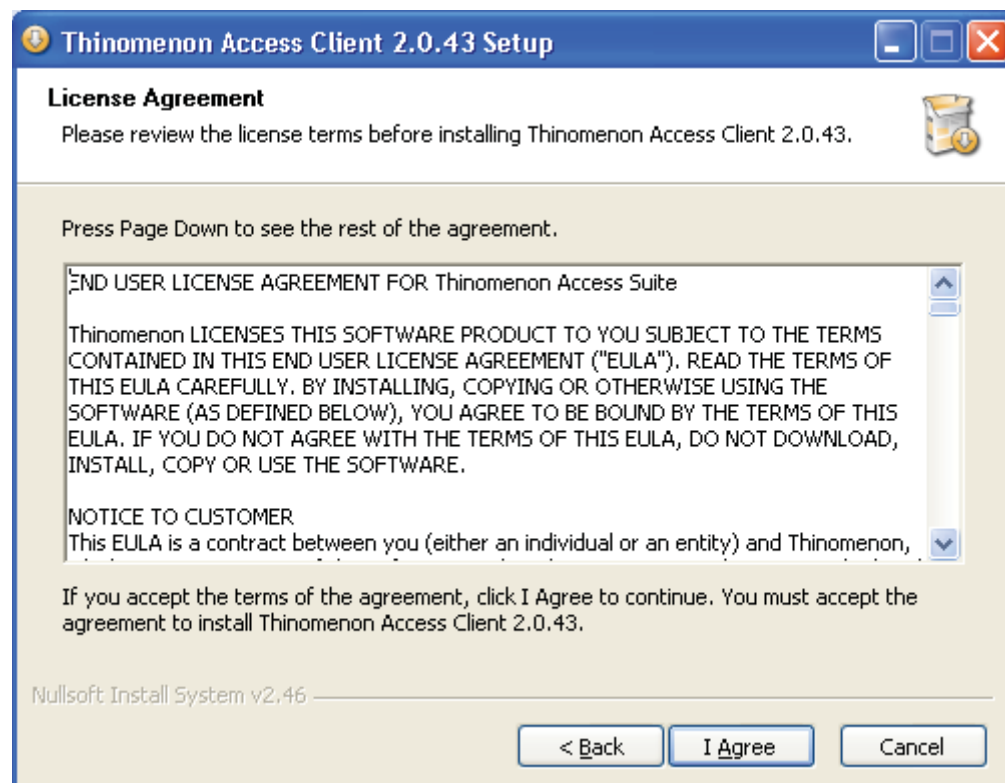
To get Access Suite Client, launch web browser on client computer, point browser to the server, where Web portal is installed, click **Download**, and save the file.



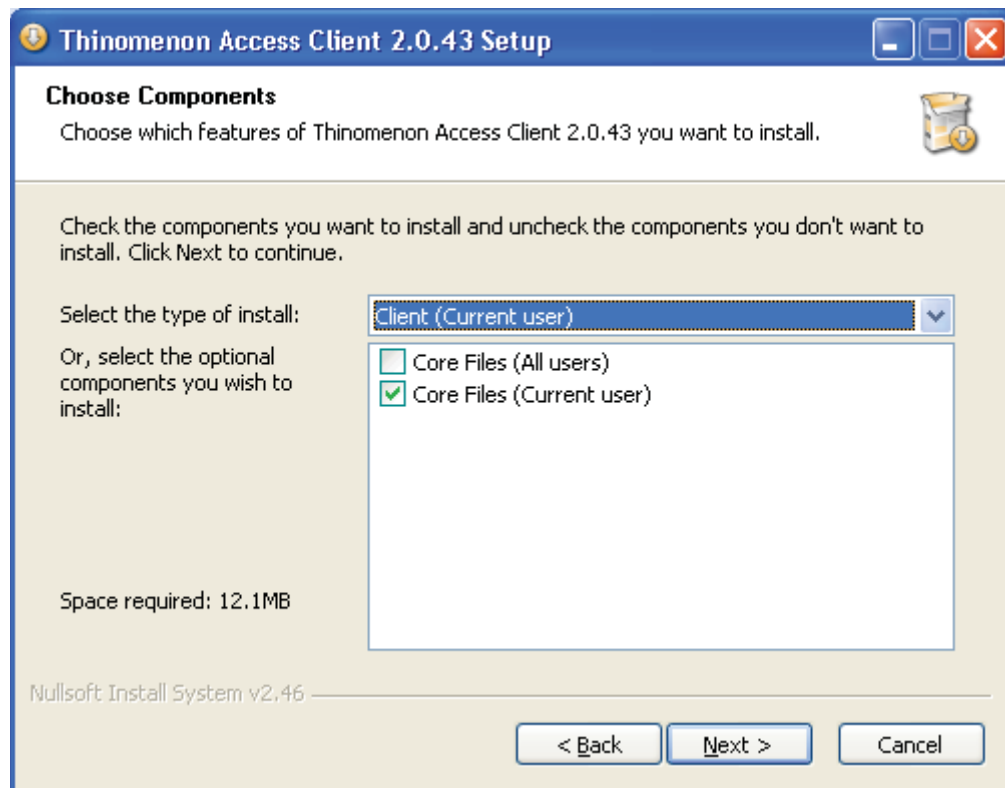
1. Launch the installer application. Once started the following window will appear:



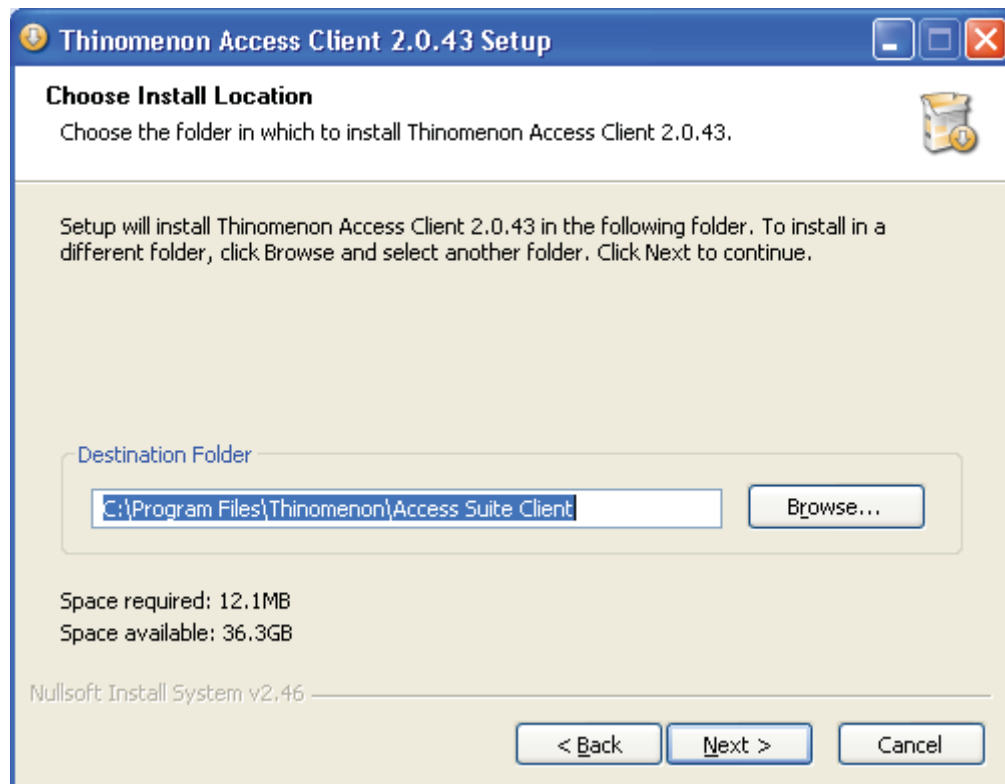
2. You will be asked to accept Thinomenon Access Suite End-User License Agreement. Please read and accept the license.



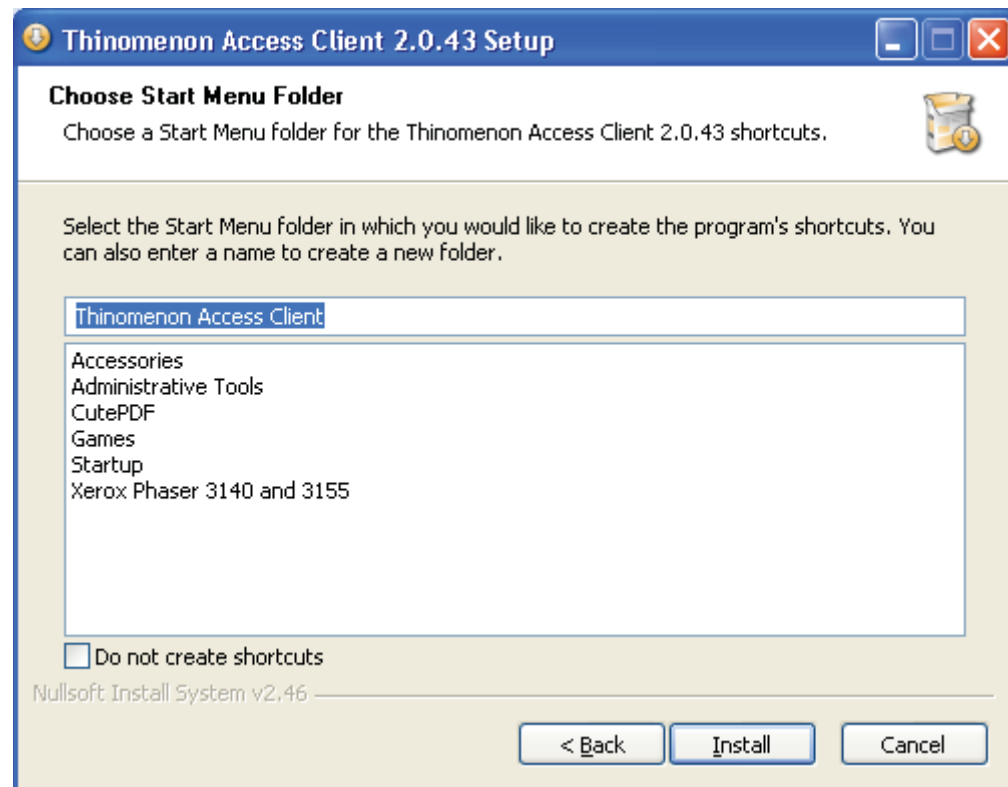
3. Choose whether Access Client will be installed for current user or for all users.



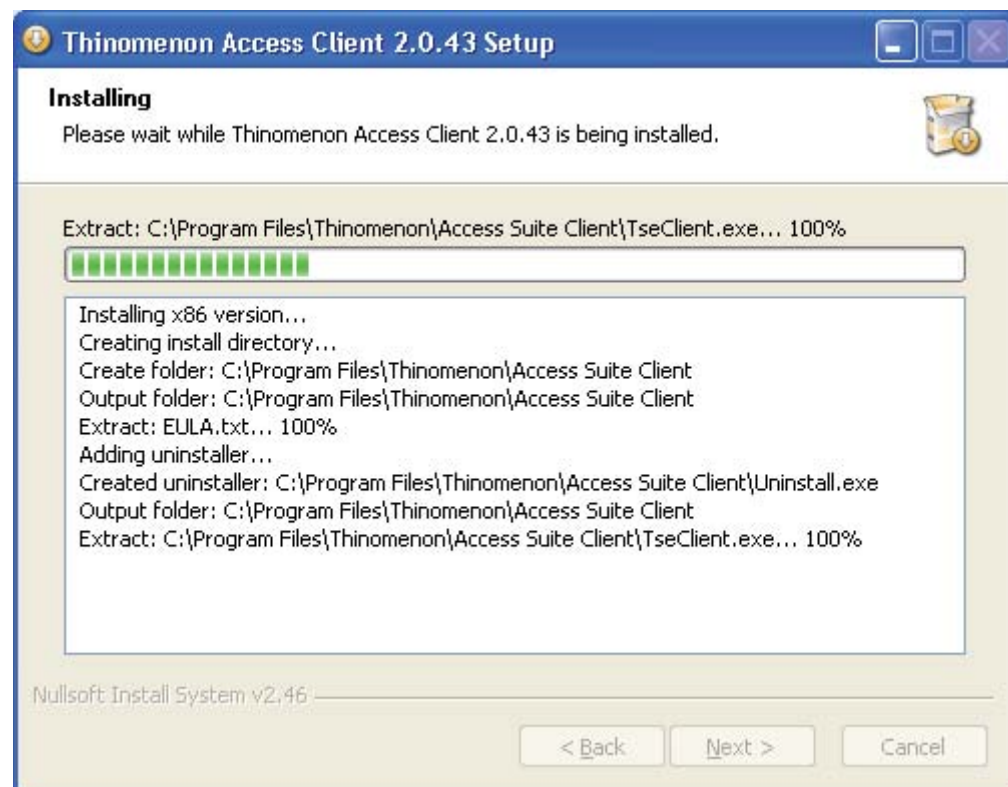
4. Choose an installation folder:



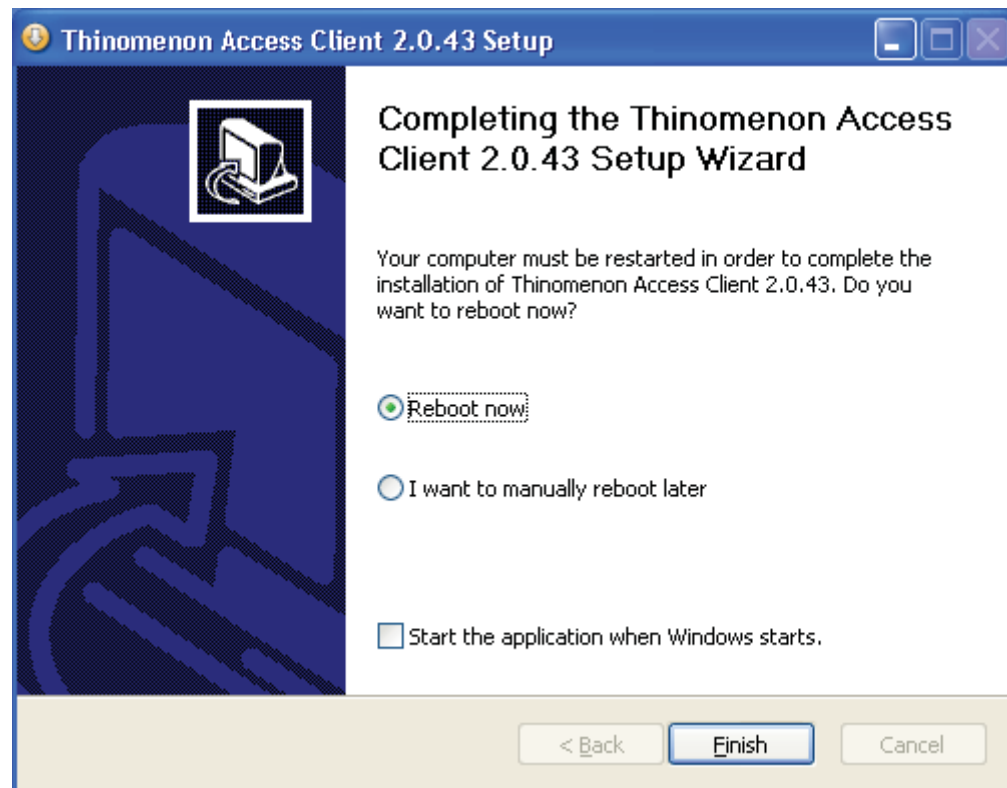
5. As the last step before setup will copy the binaries, please enter the name for the Thinomenon Access Suite program group.



6. Installation is in progress.



7. Once setup is complete, you will be asked to reboot your system.



Also you can let Thinomenon Access Client start together with OS by selecting **Start the application when Windows starts** option.

4.2.2 Managing Thinomenon Access Client wide-options

4.2.3 Enable/Disable Status Bar

To Enable or Disable Status Bar go to **View -> Status Bar**



4.2.4 Change Startup option

To Change startup options go to **Tools -> Options** menu:



4.2.5 Change Appearance option

To Change Appearance options go to **Tools -> Options** menu:



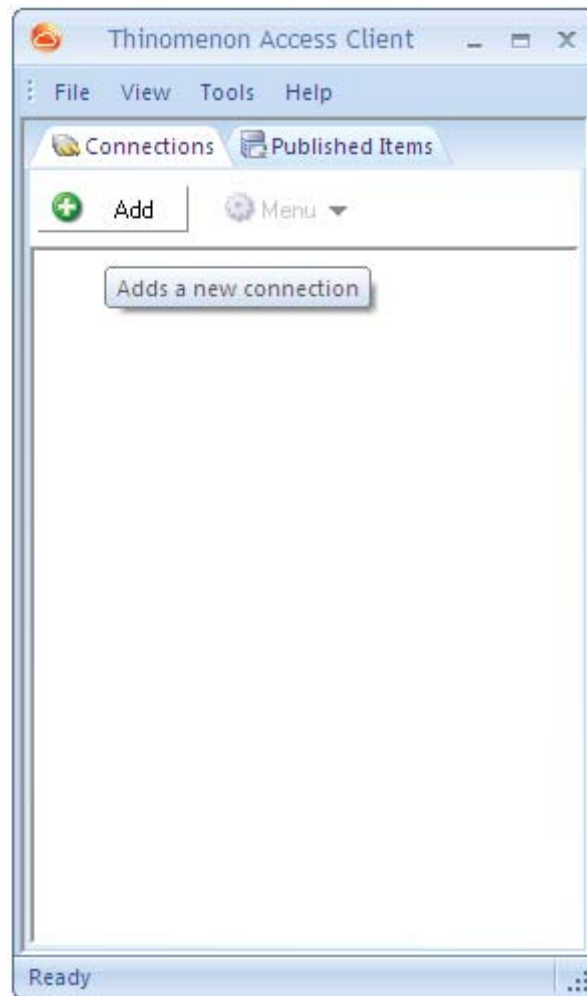
4.3 Managing Connections

4.3.1 Add a New Connection

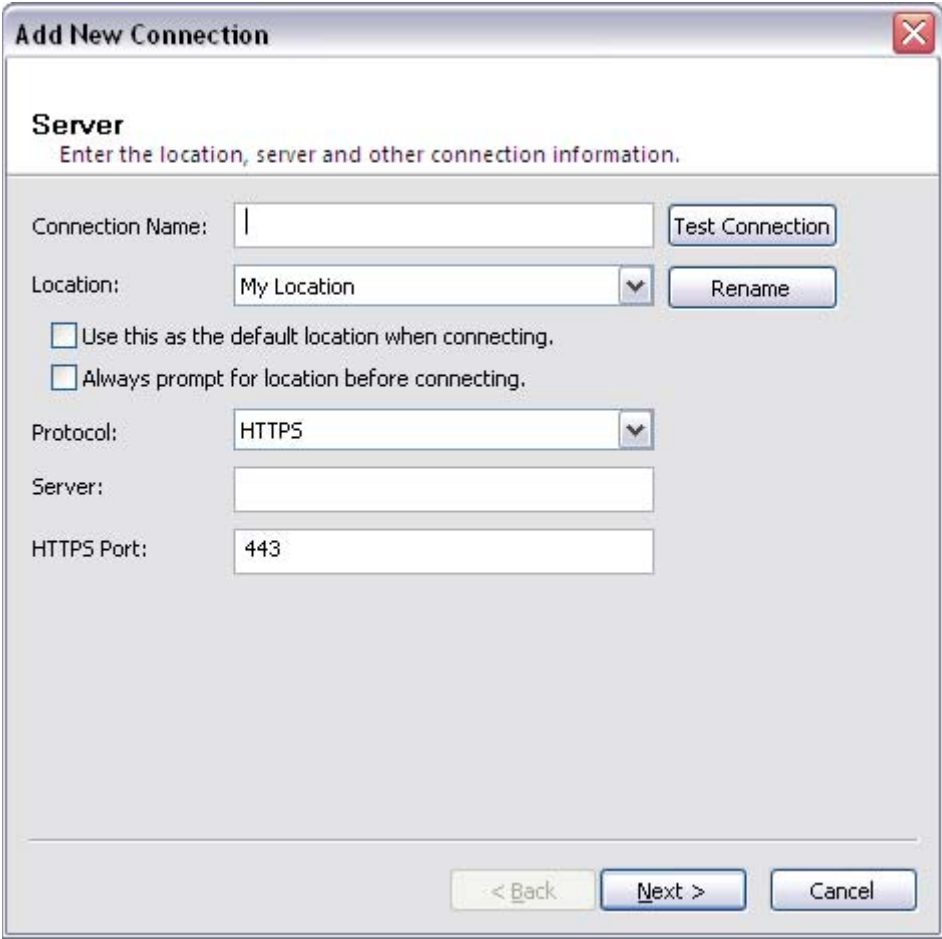
After Access Client is installed, the next step is to create connection to the server.

To add New Connection:

1. Launch Access Client. Click on **Add** button.



Add New Connection wizard appears.



2. Specify **Connection Settings**.

Then specify the Thinomenon server¹ by IP address or server's name. And specify Application Gateway's port for connection. By default it is TCP 443².

One connection can have more than one location. Each location stores the connection settings to a specific Thinomenon farm.

Use this as the default location when connecting option specifies that location, which will be used by default.

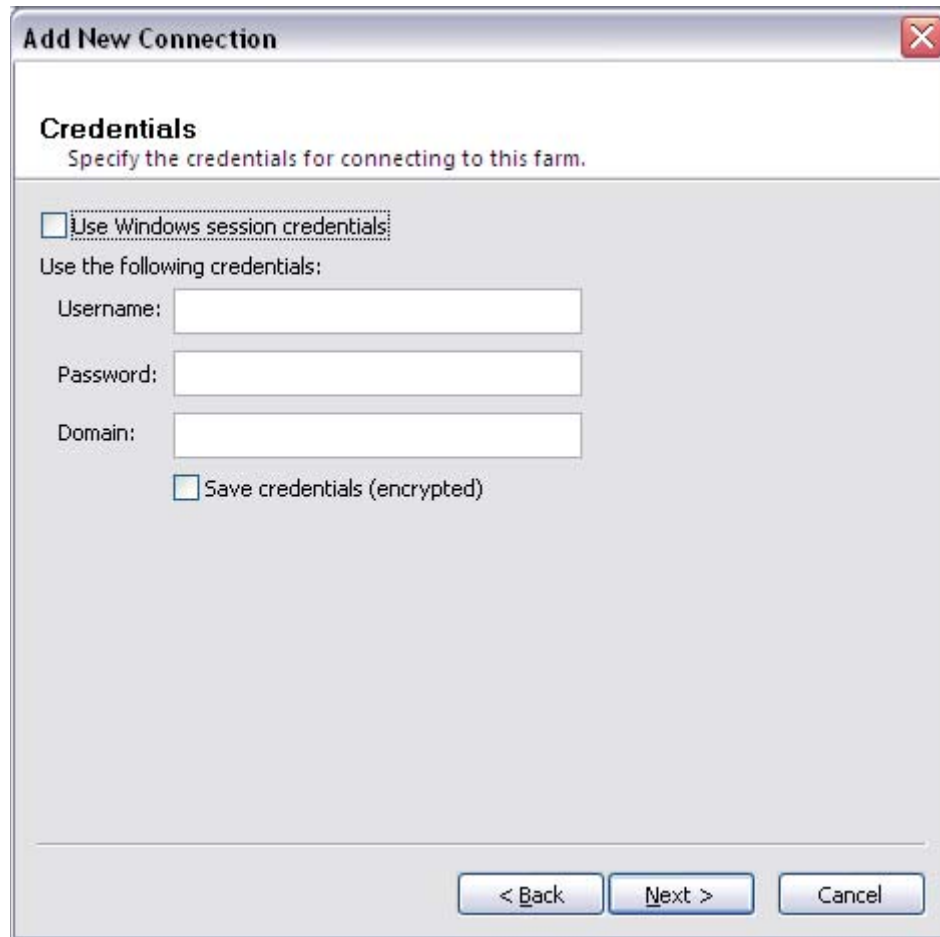
If turn on *Always prompt for location before connecting* option, user will be asked to choose a location before connect.

Click *Next*

¹ Thinomenon server – server, where Application Gateway, Enterprise Management Console and Web Portal components are installed.

² See **Components Overview** section for more details.

3. Specify credentials of domain user who is allowed to launch remote sessions from Thinomenon farm, and select whether to save the above username/password/domain.



The image shows a Windows-style dialog box titled "Add New Connection". It has a close button (X) in the top right corner. The main content area is titled "Credentials" with a subtitle "Specify the credentials for connecting to this farm." Below this, there is a checkbox labeled "Use Windows session credentials:". If this checkbox is selected, the user would be prompted to enter their Windows credentials. If it is not selected, the user is prompted to "Use the following credentials:" and is provided with three text input fields for "Username:", "Password:", and "Domain:". Below these fields is another checkbox labeled "Save credentials (encrypted)". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Use Windows session credentials option should be selected if the client computer is joined to the domain and you want to reuse the user domain credentials on the client computer to connect to Thinomenon Farm.

Click *Next*

4. Adjust display settings. Choose size of remote desktop, color depth and other display-related settings.³



5. Select the local resources you want to use in remote session: sound, printers, scanners, USB devices etc.

³ Note that there can be color depth limitations for Terminal Servers set by RDP-Tcp properties. For more details see Appendix C.

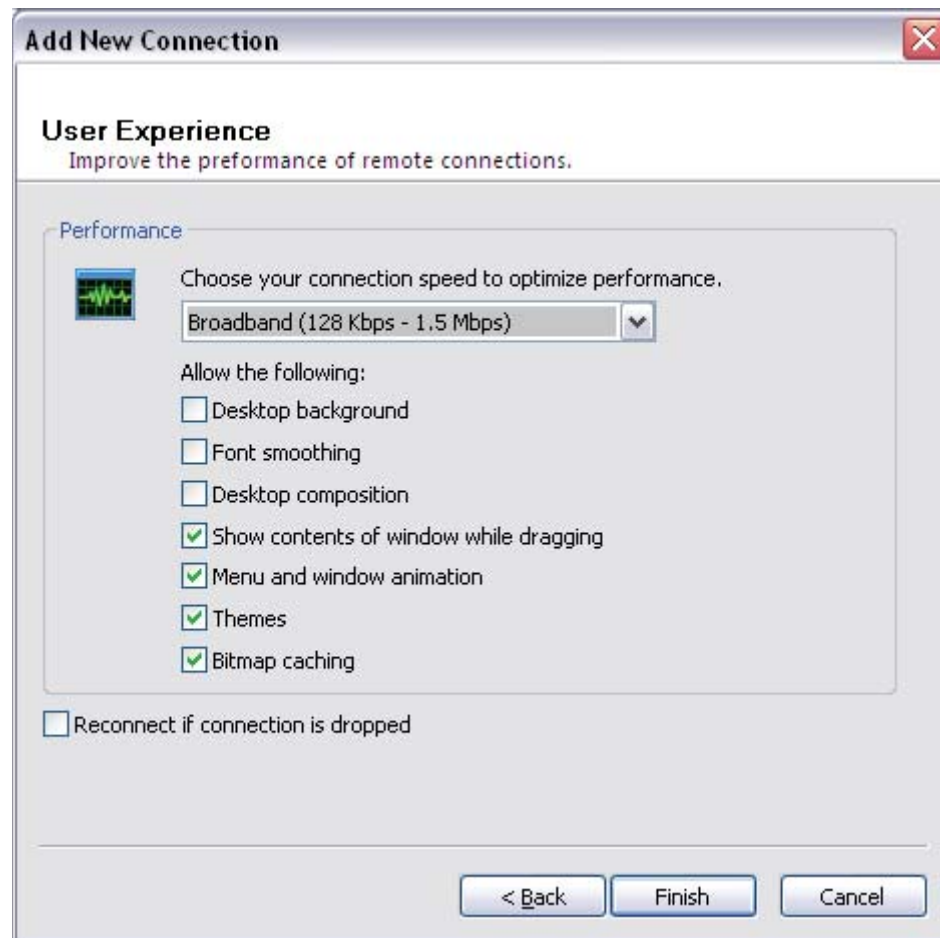


By selecting ***Bring to this computer*** option in ***Remote computer sound*** section you enable Thinomenon audio device usage in remote session.

Enable File Association option turned on means that local client files, which have extensions associated with specific published applications, will be opened with help of remote applications. This feature is useful when user doesn't have an application installed locally to work with his local files. Turning on File Associations enables Disk Drives redirection as well.

Click ***Next***

6. Defining the performance settings of remote session.



4.3.2 Modifying Connection Properties

Once connection is created, it appears on **Connections** tab.

To view and edit connection settings:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu.

The screenshot shows the 'AccUser' dialog box with the 'Server' tab selected. The dialog has a left sidebar with tabs: 'Server' (selected), 'Credentials', 'Display', 'Local Resources', and 'User Experience'. The main area contains the following fields and controls:

- Connection Name:** A text box containing 'AccUser' and a 'Test Connection' button.
- Location:** A dropdown menu showing 'My Location' and a 'Rename' button.
- Default Location:** Two checkboxes: 'Use this as the default location when connecting.' (unchecked) and 'Always prompt for location before connecting.' (checked).
- Protocol:** A dropdown menu showing 'HTTPS'.
- Server:** A text box containing '192.168.1.74'.
- HTTPS Port:** A text box containing '443'.

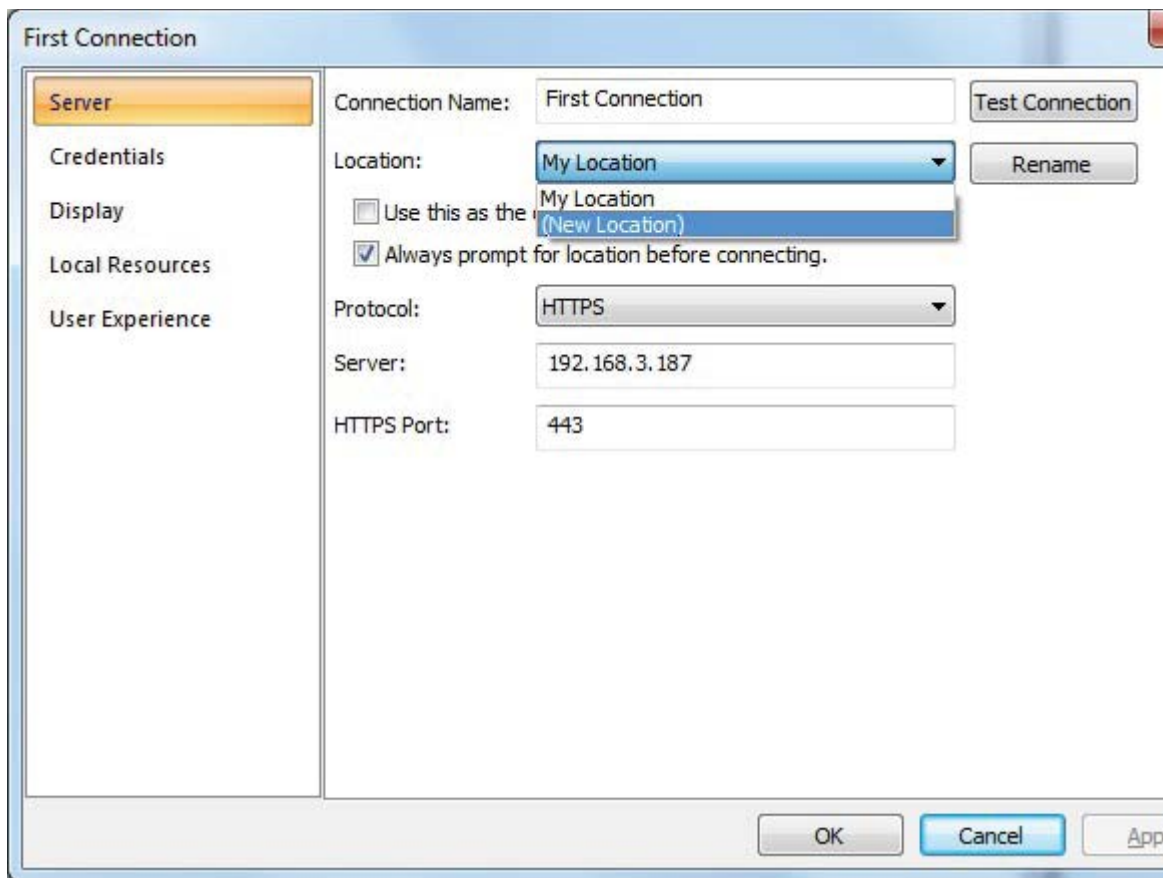
At the bottom right, there are 'OK', 'Cancel', and 'Apply' buttons.

4.3.2.1 Modifying Server Settings

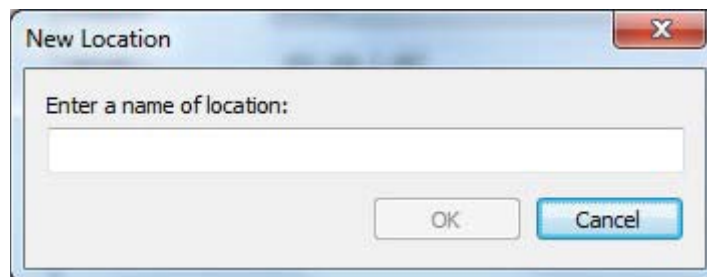
4.3.2.1.1 Add new Location

To add new Location:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Click on Location drop-down list and select New Location



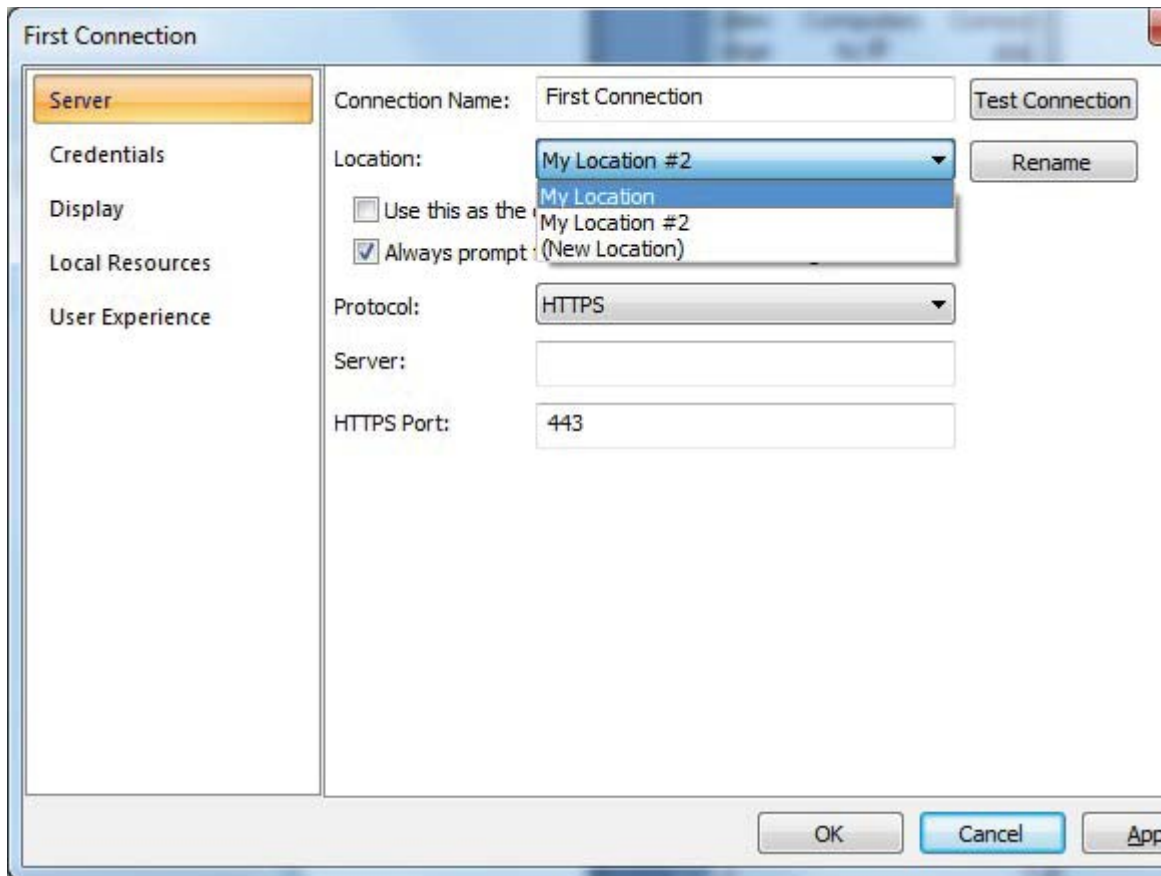
3. Specify Location name. Click **OK**



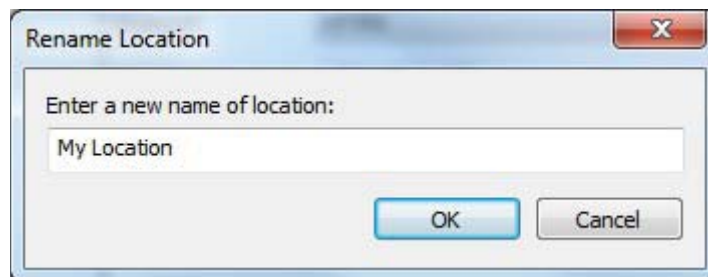
4.3.2.1.2 Rename Location

To Rename Location:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Click on Location drop-down list and select Location you want to rename



3. Click **Rename**. Rename Location window appears



3. Specify new Location name. Click **OK**

4.3.2.1.3 Specify Default Location

To Specify default Location:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Click on Location drop-down list and select Location you want to use as default
3. Check Use this as the default location when connecting option. Click **OK**

4.3.2.1.4 Enable/Disable Location Prompting before connecting

To Enable Location Prompting before connecting to server:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu

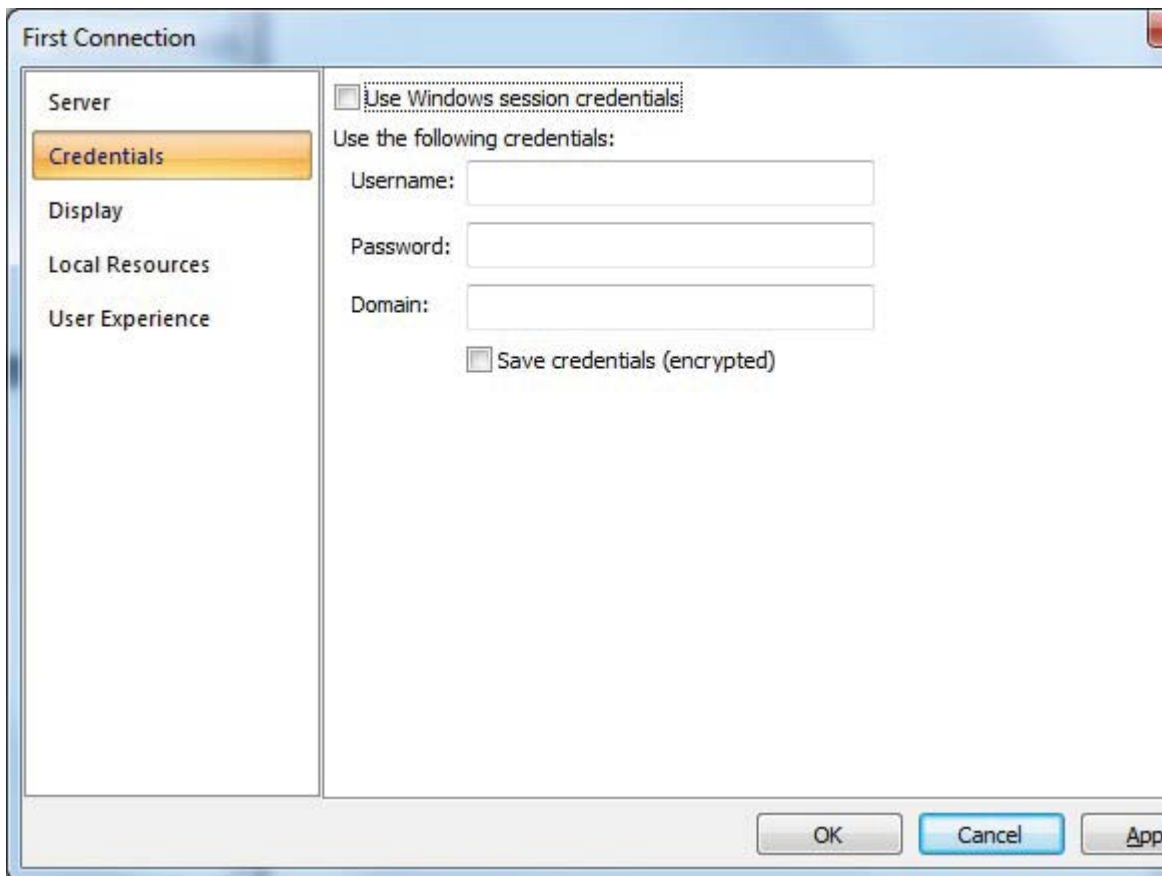
2. Check Use this as the default location when connecting option. Click **OK**

4.3.2.2 Modifying Credential Settings

4.3.2.2.1 Use Windows Session Credentials

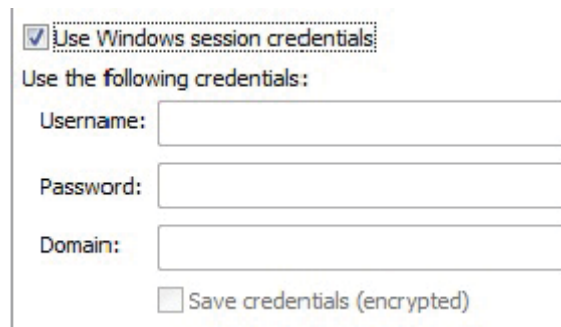
To use Windows session credentials.

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to Credentials tab.



The screenshot shows the 'First Connection' dialog box with the 'Credentials' tab selected. The left sidebar contains 'Server', 'Credentials' (highlighted), 'Display', 'Local Resources', and 'User Experience'. The main area has a checkbox 'Use Windows session credentials' which is currently unchecked. Below it, the text 'Use the following credentials:' is followed by three input fields for 'Username:', 'Password:', and 'Domain:'. At the bottom of this section is another checkbox 'Save credentials (encrypted)' which is also unchecked. At the bottom right of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

3. Check Use Windows session credentials option. Click **OK**

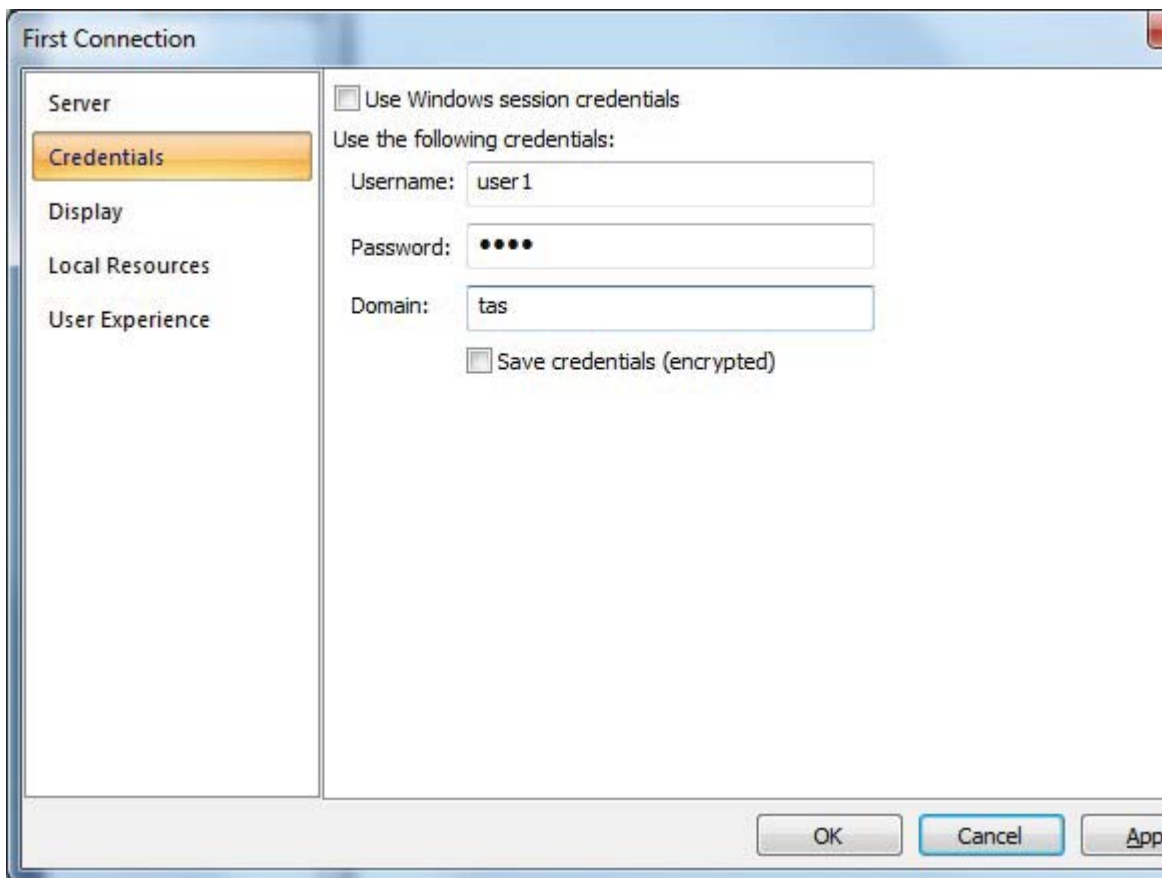


This is a close-up of the 'Use Windows session credentials' checkbox, which is now checked. The other elements (input fields and 'Save credentials (encrypted)' checkbox) remain the same as in the previous screenshot.

4.3.2.2.2 Save Credentials

To save credentials (...):

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Credentials** tab.
3. Specify credentials.



4. Check Save credentials (encrypted)

Use the following credentials:

Username:

Password:

Domain:

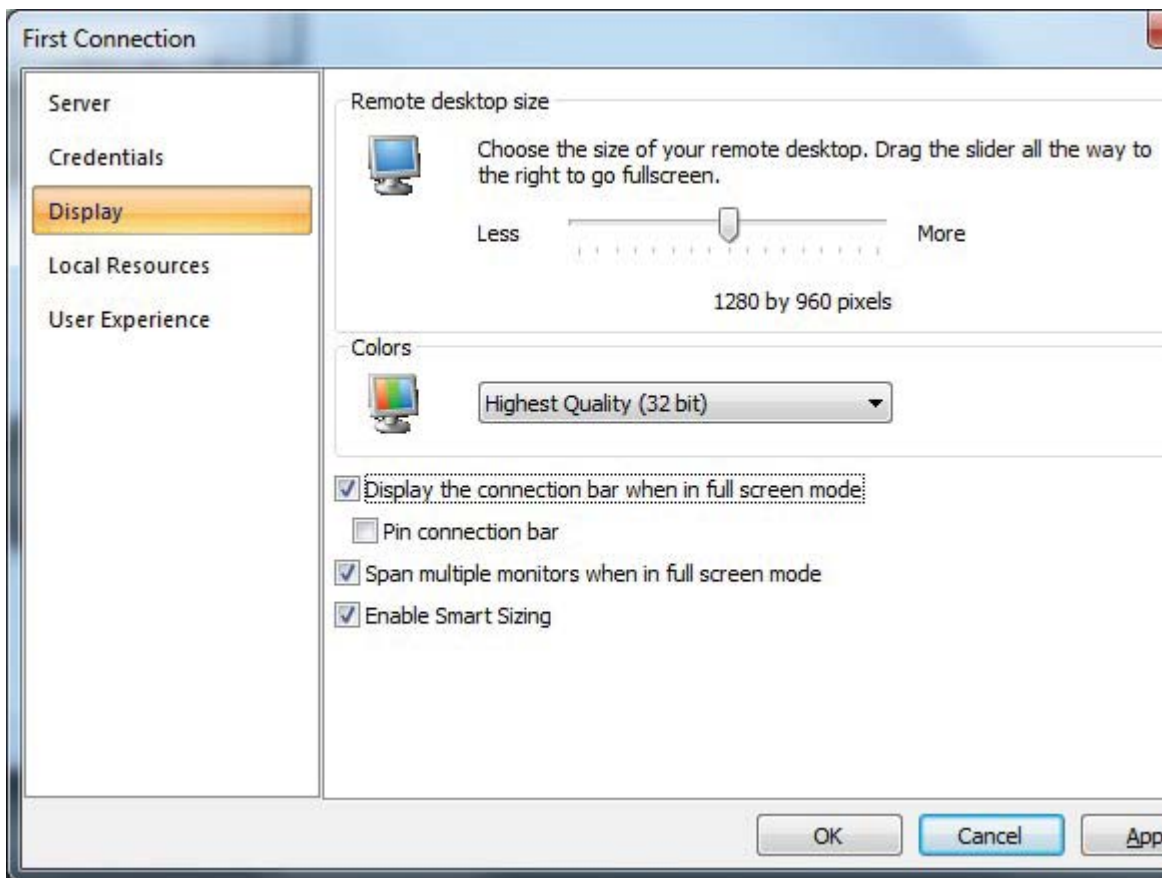
☒ Save credentials (encrypted)

4.3.2.3 Modifying Display Settings

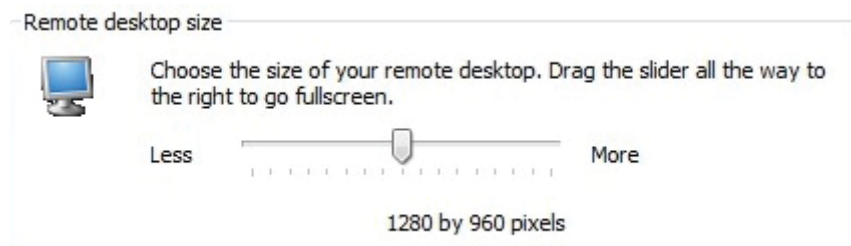
4.3.2.3.1 Change Remote Desktop size

To Change Remote Desktop size:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Display** tab.



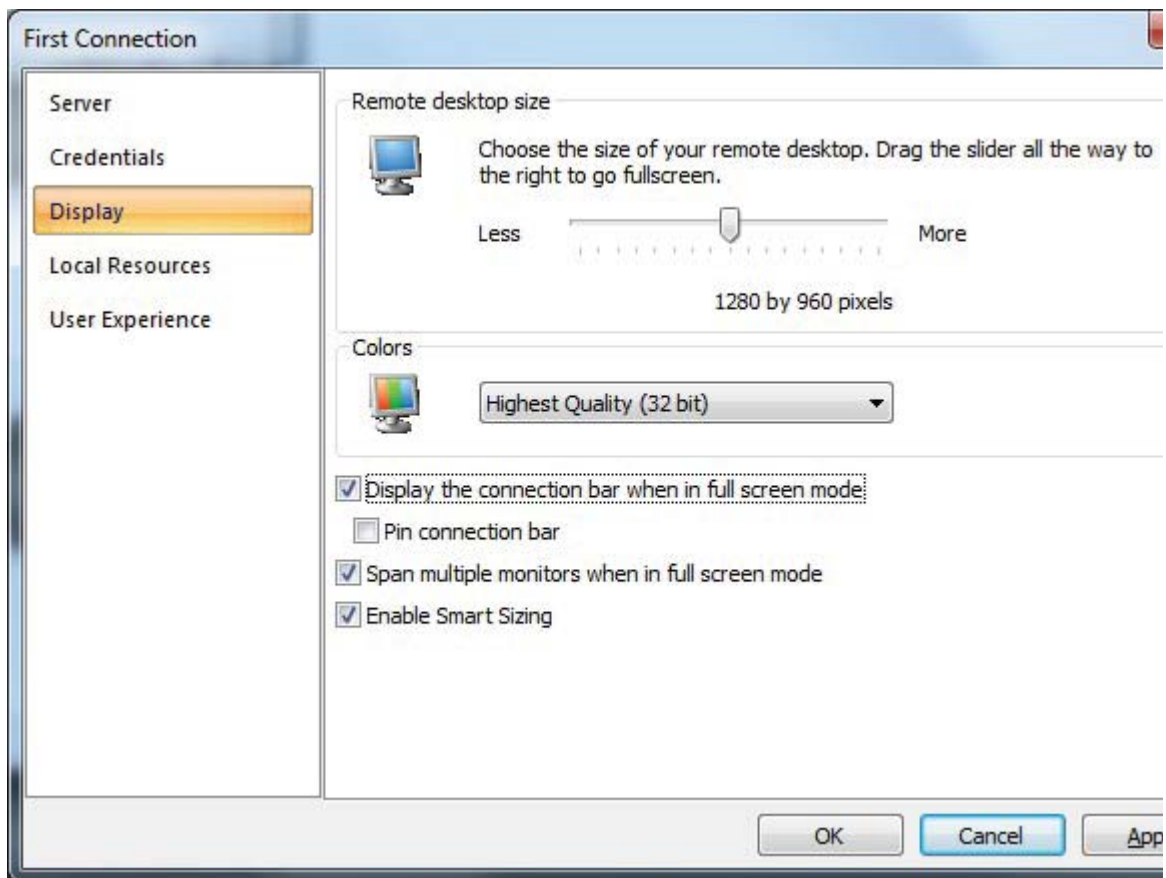
3. Choose Remote Desktop size you want to use in remote desktop session. Click **OK**



4.3.2.3.2 Change Color quality

To Change Color quality:

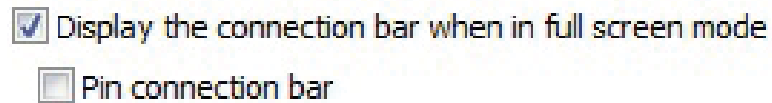
1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Display** tab.
3. Choose Color quality from drop-down list. Click **OK**



4.3.2.3.3 Change connection bar options

To Change connection bar option:

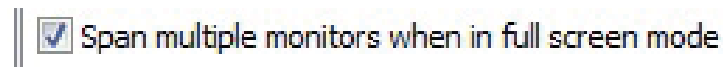
1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Display** tab.
3. Check Display the connection bar when in full screen mode option.
- 3.1 If you want to Pin connection bar – you should check Pin connection bar option. Click **OK**



4.3.2.3.4 Enable Span multiple monitors

To enable span multiple monitors when in full screen mode:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Display** tab.
3. Check Span multiple monitors when in full screen mode option. Click **OK**



4.3.2.3.5 Enable Smart Sizing

To enable Smart Sizing:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Display** tab.
3. Check **Enable Smart Sizing** option. Click **OK**

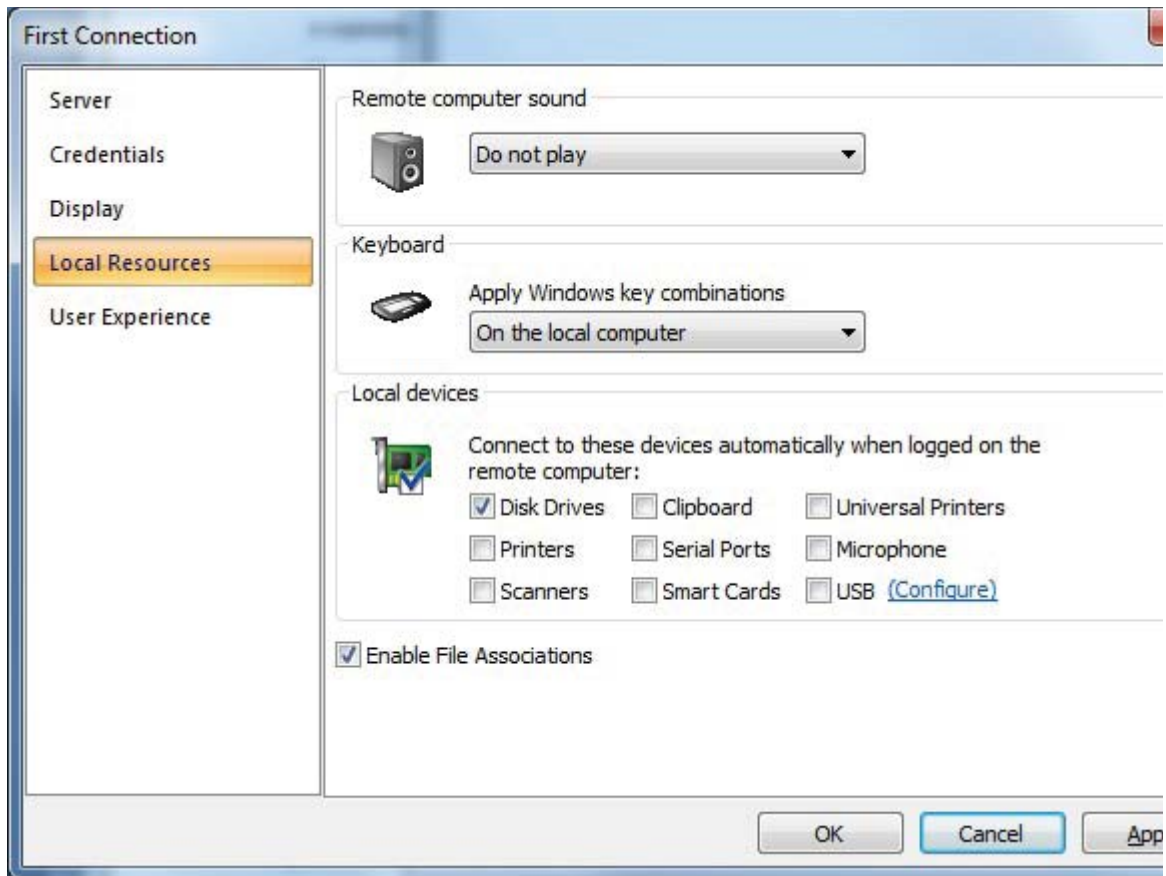


4.3.2.4 Modifying Local Resources Settings

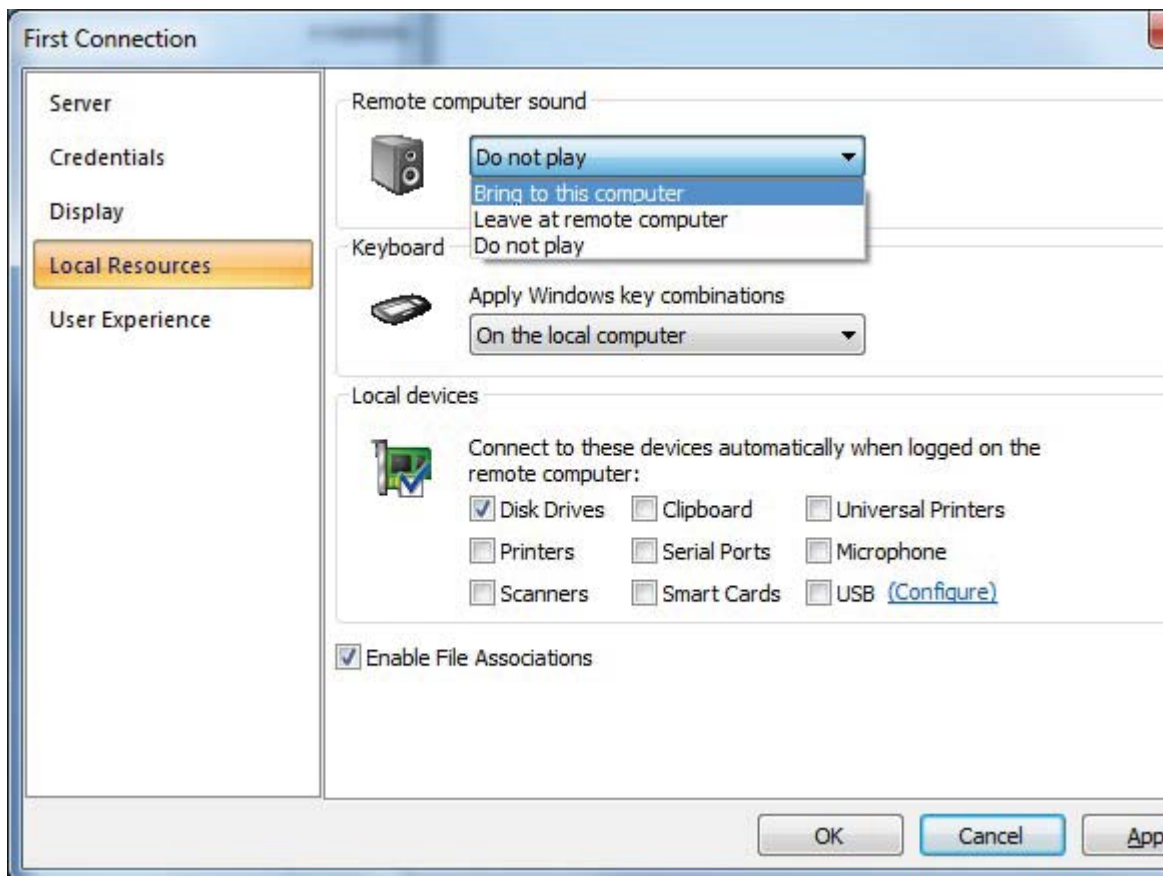
4.3.2.4.1 Change Remote computer Sound Settings

To change Remote computer sound settings:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.



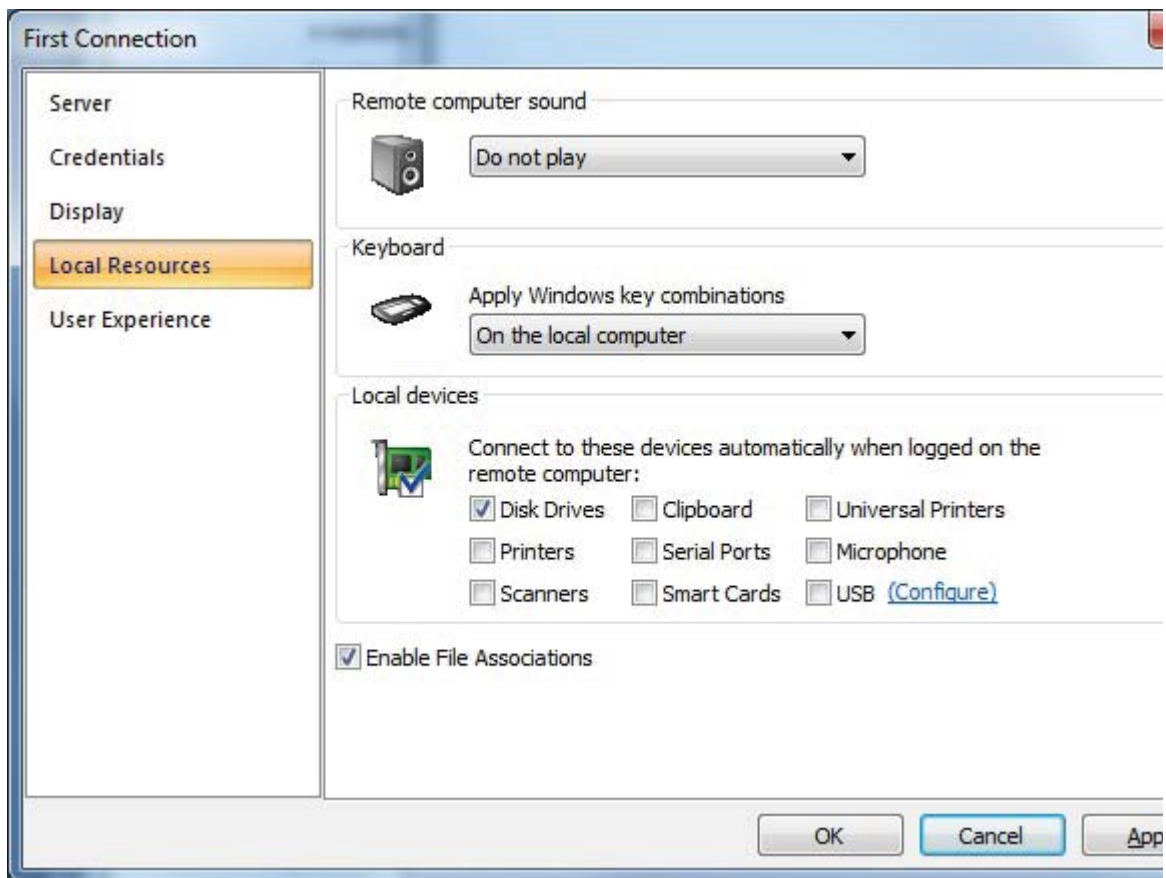
3. Select option from *Remote computer sound* drop-down list. Click **OK**



4.3.2.4.2 Change Keyboard Settings

To change Keyboard settings:

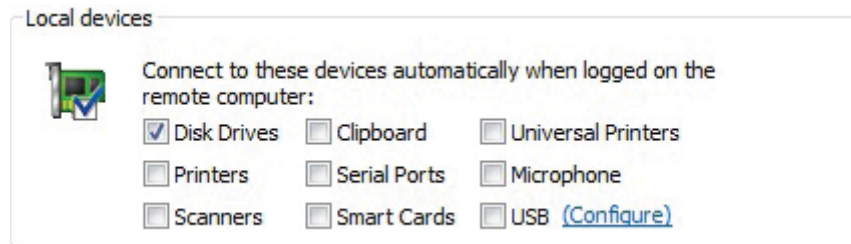
1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Select option from **Keyboard** drop-down list. Click **OK**



4.3.2.4.3 Modify Devices Redirection

To modify Local devices which will be redirected to remote session:

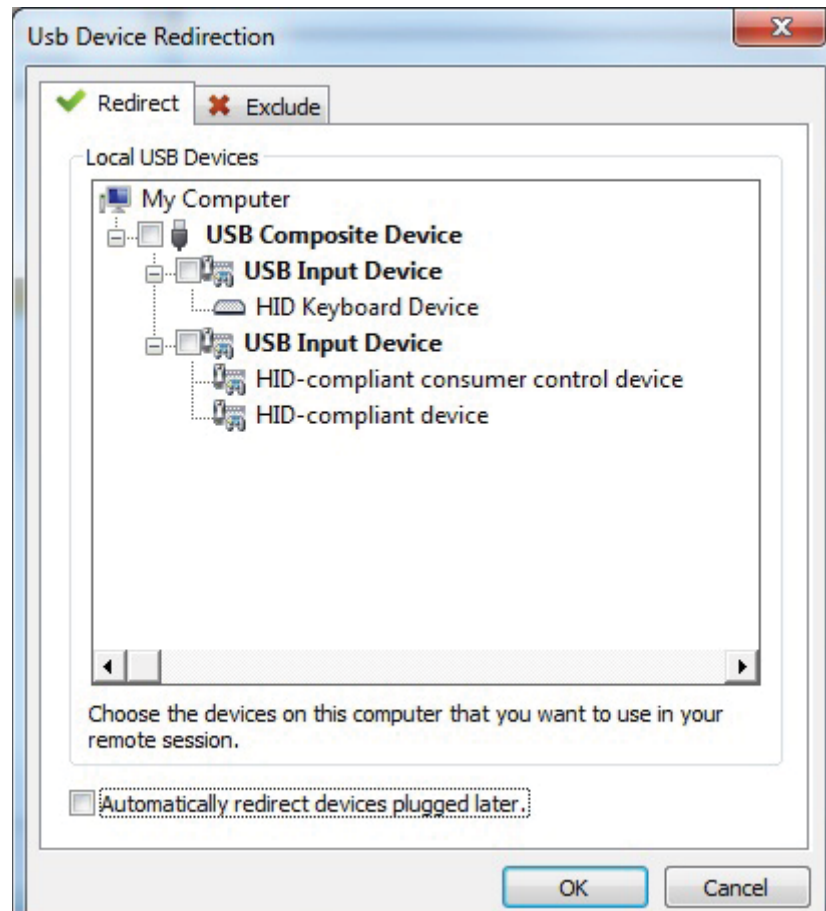
1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Check Devices you want to redirect to remote session. Click **OK**



4.3.2.4.4 Modify USB Redirection tab

To modify USB Redirect tab:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Click **Configure** link that is near USB checkbox.

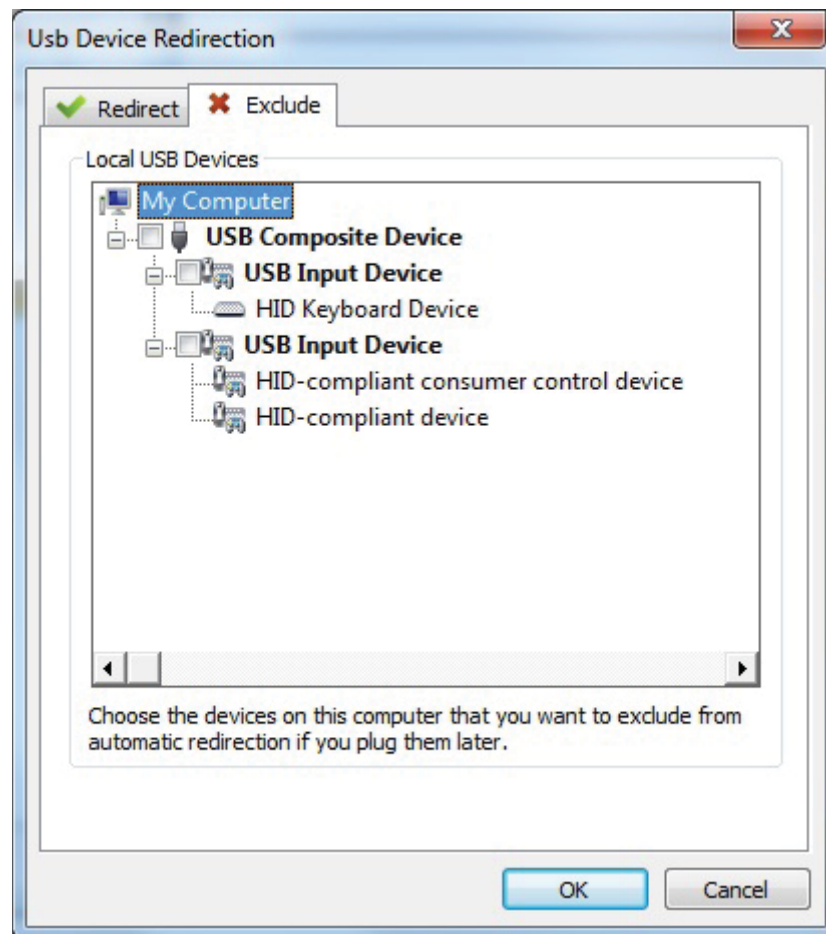


4. Select USB devices which are will be redirected to remote session. Click **OK**

4.3.2.4.5 Modify USB Exclude tab

To modify USB Exclude tab:

1. Select **Menu -> Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Click **Configure** link that is near USB checkbox.
4. Go to **Exclude** tab

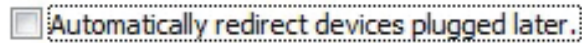


5. Select USB devices which are will not be redirected to remote session. Click **OK**

4.3.2.4.6 Enable Automatically Redirection devices plugged later

To Enable Automatically Redirection devices plugged later:

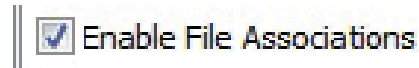
1. Select **Menu -> Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Click **Configure** link that is near USB checkbox.
4. Check **Automatically redirect devices plugged later** option. Click **OK**



4.3.2.4.7 Enable File Associations

To Enable File Associations:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **Local Resources** tab.
3. Check **Enable File Associations** option. Click **OK**

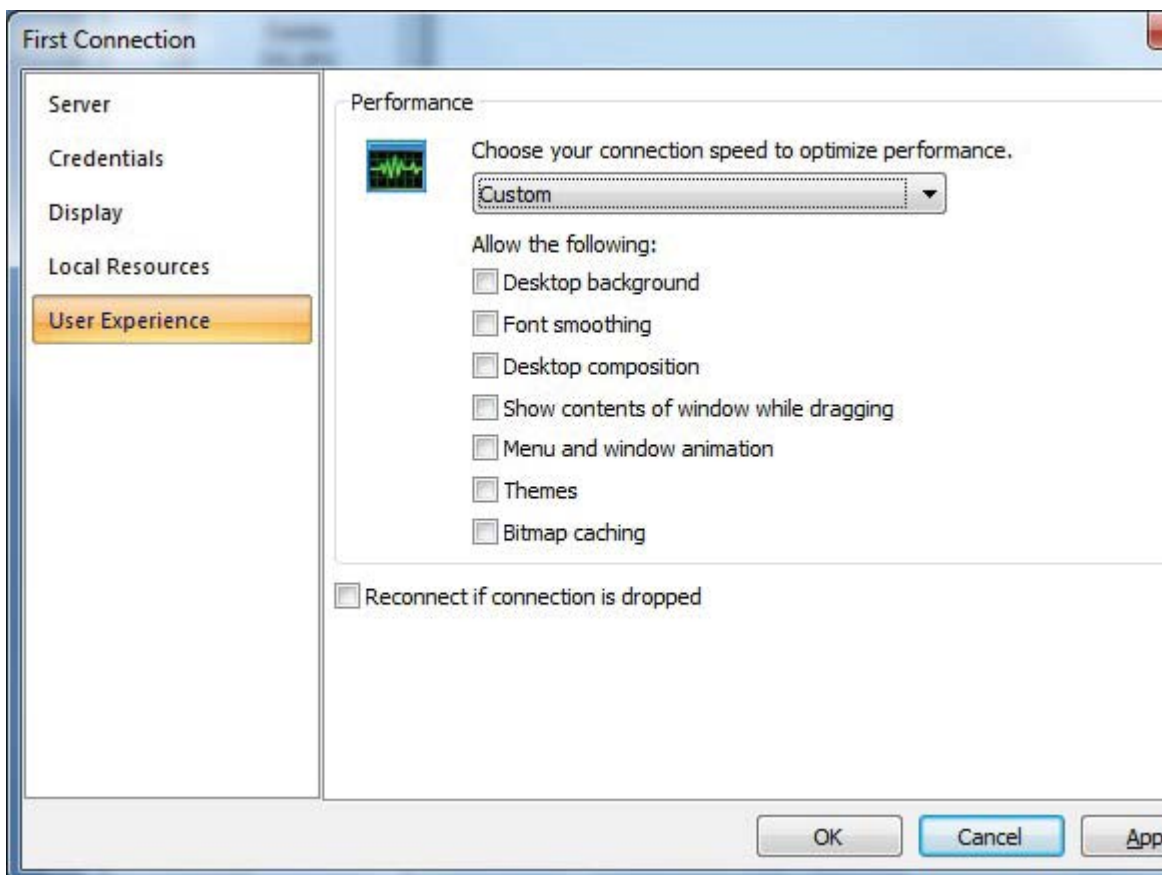


4.3.2.5 Modifying Performance Settings

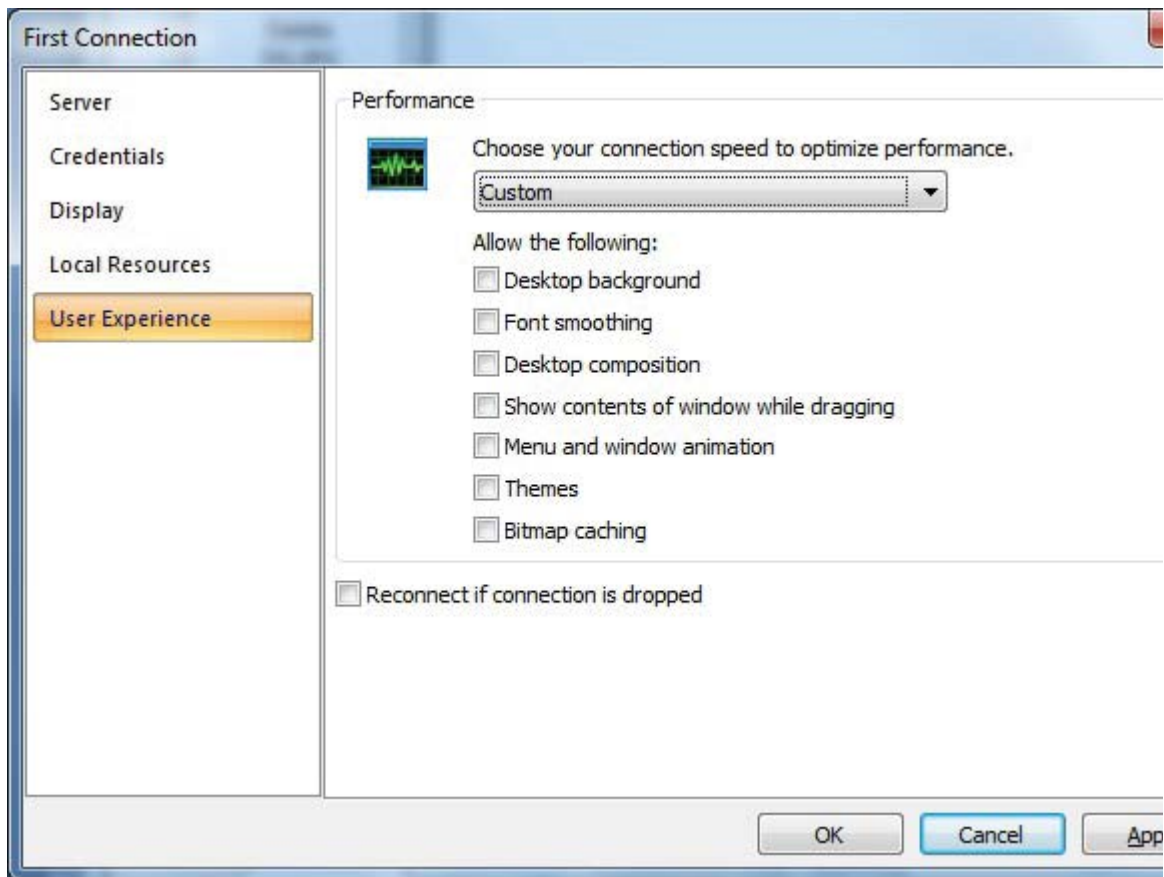
4.3.2.5.1 Change connection speed to optimize performance

To change connection speed:

1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **User Experience** tab.



3. Select option from drop-down list or select options you want to allow manually.
Click **OK**



4.3.2.5.2 Enable Reconnection if connection is dropped

To enable Reconnection if connection is dropped:

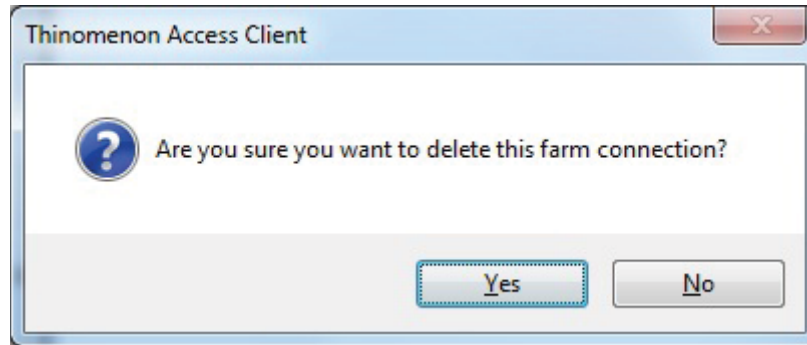
1. Select **Menu** -> **Edit** or **Edit** from connection's right-click menu
2. Go to **User Experience** tab.
3. Check **Reconnect if connection is dropped** options. Click **OK**

☐ Reconnect if connection is dropped

4.3.3 Delete Connection

To enable Reconnection if connection is dropped:

1. Select **Menu** -> **Delete** or **Delete** from connection's right-click menu
2. **Confirmation Window** appears

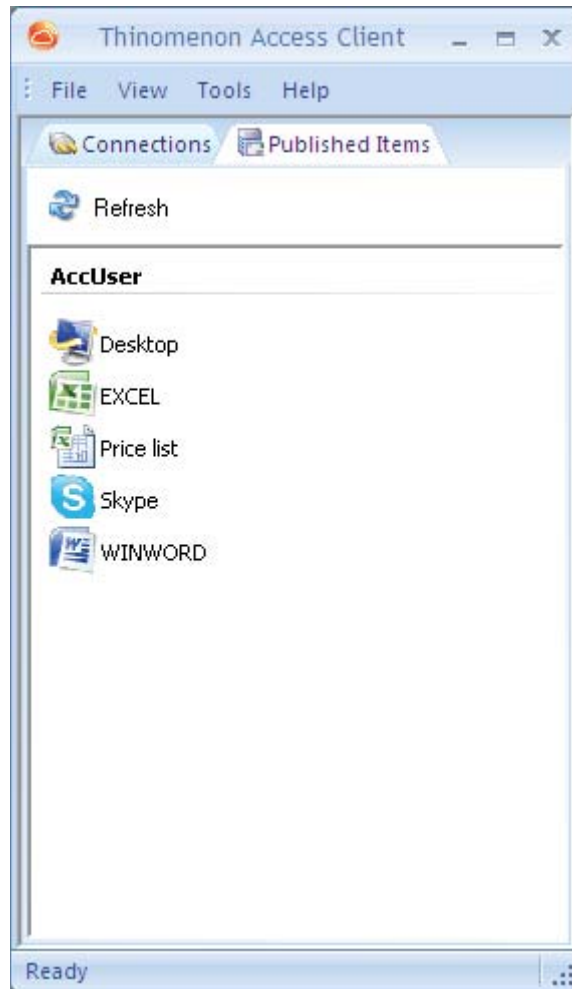


3. Click **Yes** if you sure you want to delete connection

4.4 Working with Published items

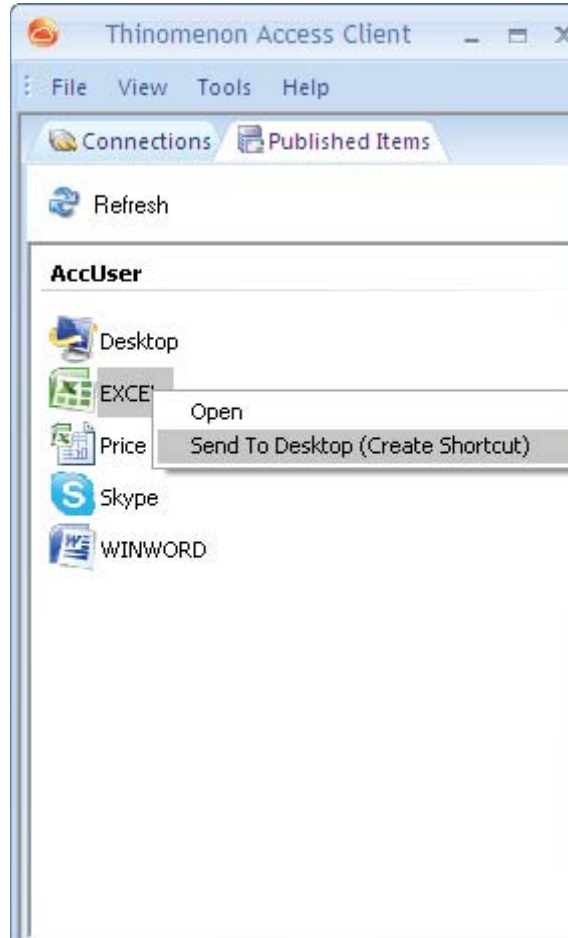
4.4.1 Starting remote connection to published items

Users can start remote connections to published desktops and applications by double-clicking the corresponding shortcuts.



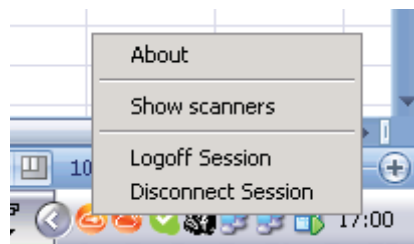
4.4.2 Create Shortcut of published items

There is an option in Access Client to create shortcut of published item and send this shortcut to desktop. To use it, right-click the specific published item and select **Send To Desktop (Create Shortcut)** item or just drag and drop this item.



4.4.3 Logoff/Disconnect sessions

After you've launched published application or document from client device, Thinomenon icon appears in system tray on client and allows to logoff or disconnect session, and to display info about available scanners.

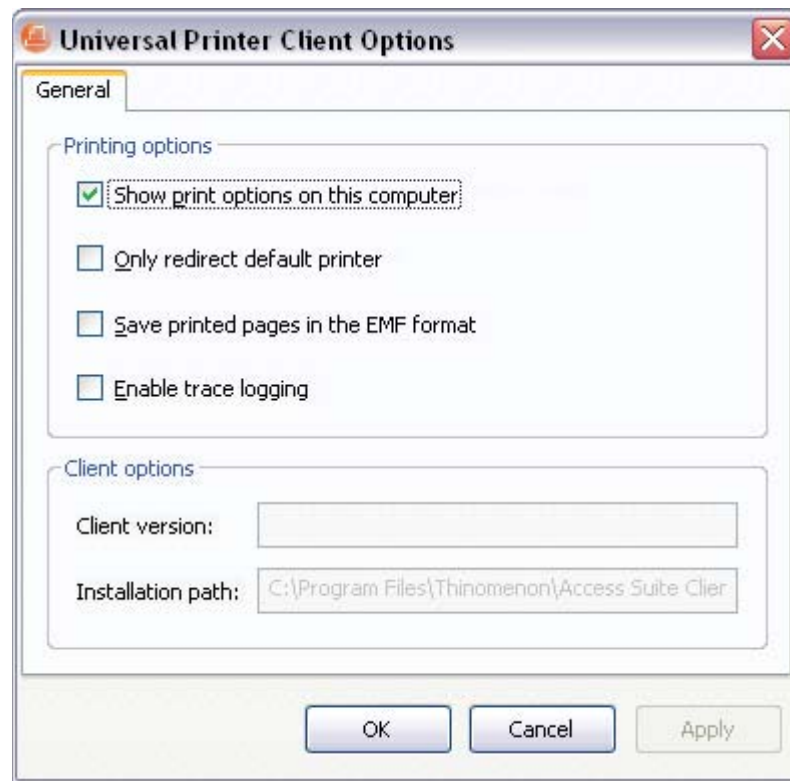


Also tray serves to display error messages.

If case of full desktop session, Thinomenon tray icon appears in remote desktop session.

4.5 Managing Universal Printer Client options

After Access Client installation Universal Printer applet appears in Control Panel:



The following options can be set from Universal Printer Client Options dialog.

4.5.1 Enable Show Print options on this computer

Show print options on this computer – turn on/off displaying of dialog with print options on client side each time after some document was sent to print. Changes according to this option are applied next time you print with help of Universal Printer.

To enable Show print options on this computer:

1. Open **Universal Printer Client Options** from **Control Panel**
2. Check Show print options on this computer option. Click **OK**

4.5.2 Only redirect default printer

Only redirect default printer – only default client's printer will be redirected to session. Changes according to this option are applied next time you launch a remote session.

To enable redirection of default printer only:

1. Open **Universal Printer Client Options** from **Control Panel**
2. Check Only redirect default printer option. Click **OK**

4.5.3 Save Printed pages in the EMF format

Save printed pages in the EMF format – this option allows storing printed pages in EMF format to *INSTALLDIR\DumpMetaFiles\filename.emf*, where *INSTALLDIR* is the folder where Access Client was installed. Changes according to this option are applied next time you print with help of Universal Printer.

To enable saving printed pages in the EMF format:

1. Open *Universal Printer Client Options* from *Control Panel*
2. Check Save printed pages in the EMF format option. Click **OK**

4.5.4 Enable trace logging

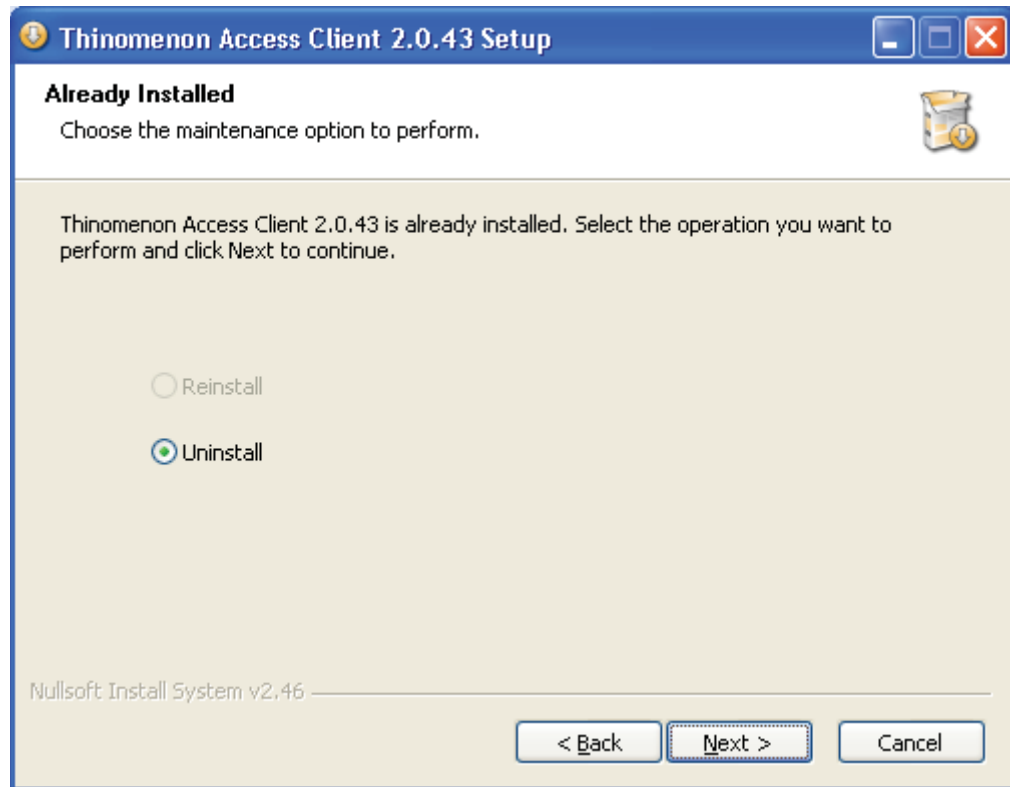
Enable trace logging – turn on/off logging for client part of Universal Printer. Changes according to this option are applied immediately. Log will be saved to *INSTALLDIR\UPrinter.log*, where *INSTALLDIR* is a directory where Member Server was installed.

To enable trace logging:

1. Open *Universal Printer Client Options* from *Control Panel*
2. Check Enable trace logging option. Click **OK**

4.6 Uninstalling Thinomenon Access Suite client

Access Client could be removed from the system by invoking the uninstaller either from Add/Remove Programs application or by directly running uninstaller application from Start -> Thinomenon Access Client -> Uninstall.



Before the removal process begins, a user has to confirm that he/she wishes to uninstall the software

5 Glossary

D

Datacenter –this is node in Thinomenon Enterprise Management Console for storing and management of virtualization servers (hypervisors). Also “datacenter” can stand for hypervisor (VMware ESXi, Microsoft Hyper-V), hypervisor manager (vCenter, SCVMM) or server with Parallels Virtuozzo Containers.

Desktop Group – it’s an entity in Thinomenon Farm, where managed computers (virtual or physical) are stored. Desktop Groups can represent an organizational structure.

DHCP (Dynamic Host Configuration Protocol)– is a network configuration protocol for hosts on Internet Protocol (IP) networks, which provides an IP address, and a default route and routing prefix.

F

Farm-node – the first node in the navigation pane represents the Thinomenon infrastructure.

Firewall - either hardware or software system limiting network access. Normally, a Firewall is deployed between a trusted, protected network and an untrusted network or computer.

H

Hypervisor – it’s software allowing multiple operating systems to share a single physical computer.

L

Load Evaluator – it’s a parameter or combination of parameters (CPU usage, memory usage etc), which is used to define server’s load. Load Evaluator is necessary for smart load balancing.

M

Microsoft Hyper-V - is a hypervisor-based virtualization system for x86-64 system. Hyper-V exists in two variants: as a stand-alone product called Microsoft Hyper-V Server 2008, and as an installable role in Windows Server 2008 R2 and Windows Server 2008.

P

Parallels Virtuozzo Containers - is an operating system virtualization solution which allows using single physical server to run multiple isolated copies of operating system (containers).

Parent VHD – it’s a virtual hard disk, which is used as basis for creation of virtual machines with linked clone method.

PDA - Personal Digital Assistant, a handheld device that combines computing,

telephone and Internet and networking features. See also Smartphone.

Promiscuous mode - is a mode for a network interface controller (NIC) that causes the NIC to pass all traffic it receives to the central processing unit (CPU) rather than just passing frames the NIC is intended to receive.

R

RDP – Remote Desktop Protocol, a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to another computer.

S

SCVMM - part of Microsoft's System Center line of management and reporting tools, designed for management of large numbers of Virtual Servers based on Microsoft Virtual Server and Hyper-V.

Smartphone – same as PDA.

Sysprep - is the name of Microsoft's System Preparation Utility for Microsoft Windows operating system deployment.

T

Terminal Server – software or hardware that allows the operation of applications from other computers, which can be in other locations.

V

VDI – it is the practice of hosting a desktop operating system within a virtual machine (VM) running on a hosted, centralized or remote server.

VDI Guest Tools – it's extensions for virtual desktops and physical computers, providing features and management functionality for managed computers.

Virtual Template – virtual machine selected on hypervisor as a template for other virtual machines to be cloned from it with help of Enterprise Management Console.

VMware vCenter - solution which centrally manages VMware vSphere environments allowing IT administrators improved control over the virtual environment.

VMware ESXi - bare-metal embedded hypervisor, VMware's enterprise software hypervisor for servers that run directly on server hardware without requiring an additional underlying operating system.

6 Appendix A

Promiscuous mode

Network Interface Controller (NIC) has a mode when it accepts all the network traffic. It's called promiscuous mode. Obtaining IP addresses via DHCP by PVC containers depends on whether promiscuous mode is enabled or not on hypervisor, where PVC virtual machine is running.

Let's see how to enable promiscuous mode on different hypervisors.

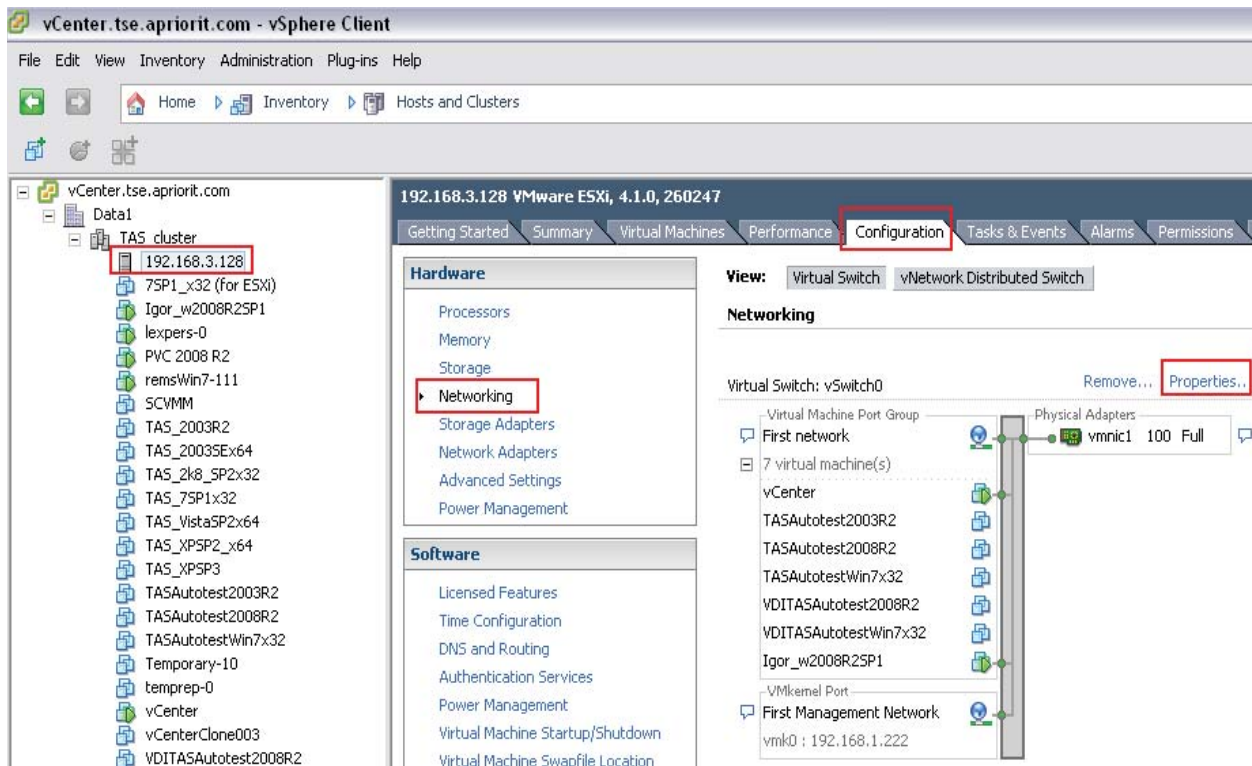
Parallels Server Bare Metal

If PVC is running on Parallels Server Bare Metal hypervisor perform the following command for PVC virtual machine from hypervisor:

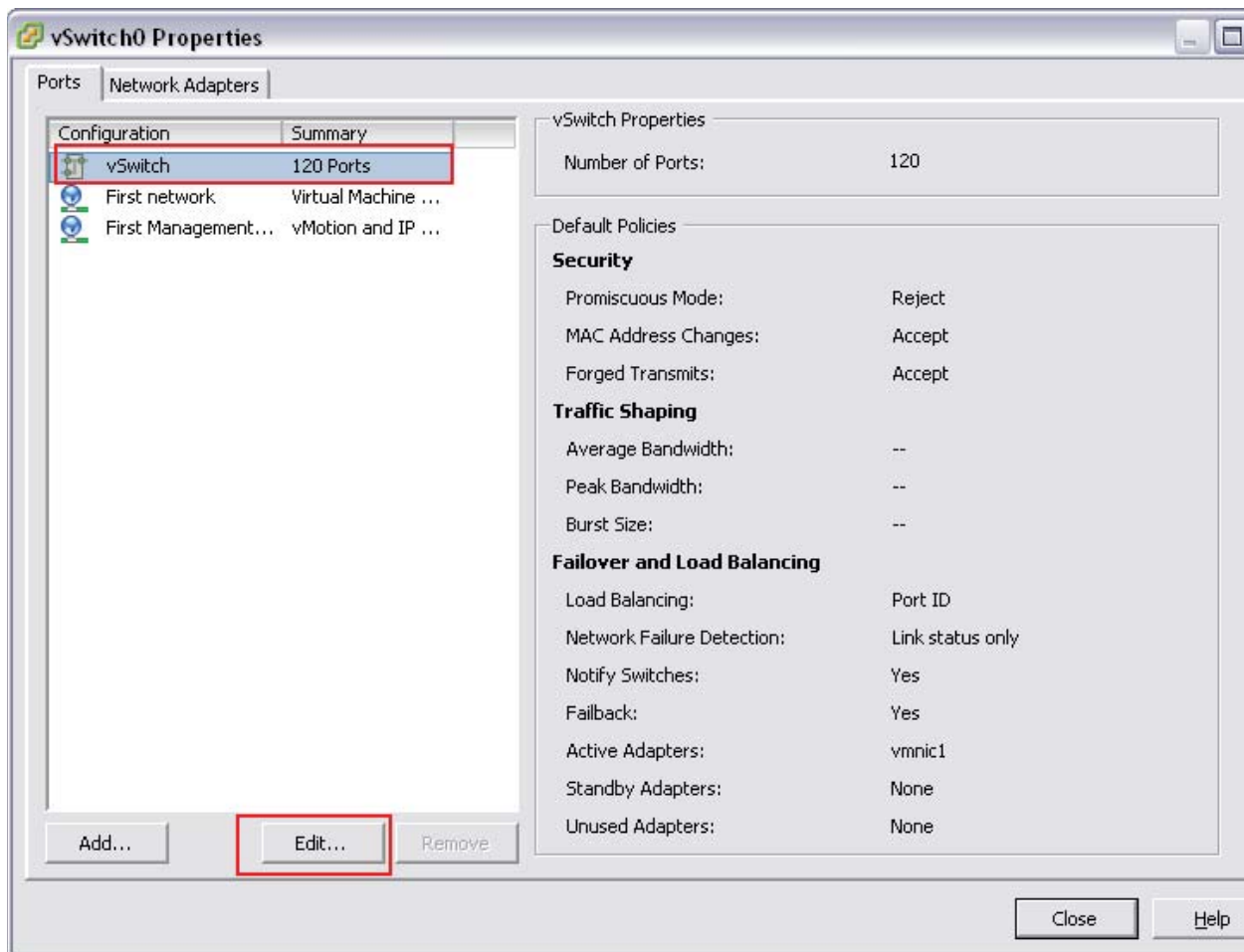
```
ptcl set "PVC VM name" --device-set net0 --preventpromisc no --ipfilter no --macfilter no
```

VMware ESXi/ VMware vCenter

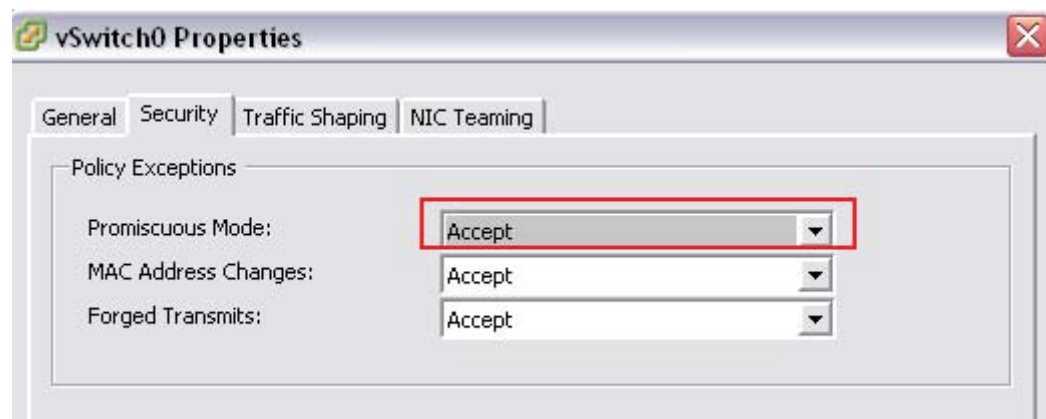
If PVC is running on ESXi hypervisor (it can be managed by vCenter or not), to enable promiscuous mode launch VMware vSphere Client, select ESXi, where PVC virtual machine is running, and open **Configuration** -> **Networking**. Select appropriate vSwitch and open its **Properties**.



In *Properties* windows select vSwitch and click *Edit*



Go to *Security* tab and select *Accept* in *Policy Exceptions* -> *Promiscuous mode*.



7 Appendix B

VMware Virtual Disk Development Kit (VDDK)

To add VMware ESXi/VMware vCenter datacenter to Enterprise Management Console, VMware Virtual Disk Development Kit (VDDK) must be installed on the server, where Management Console is hosted.

After VDDK is installed the path to VDDK bin directory must be added to the PATH environment variable.

To do this open **System Properties** window (for example, by selecting **Properties** item from **My Computer** right click menu) and go to **Advanced** tab, click **Environment Variables** button, select **Path** variable among system variables, click on Edit button and append full path to VDDK bin directory.

For example, C:\Program Files\VMware\VMware Virtual Disk Development Kit\bin

It is recommended to install VDDK before Thinomenon Management Console installation. Otherwise (if Thinomenon Access Suite server was installed prior to VDDK) you need to register EsxProvider.dll manually.

You can do it from Windows command line interface. Click Start then Run and type the letters CMD. In the command line interface enter:

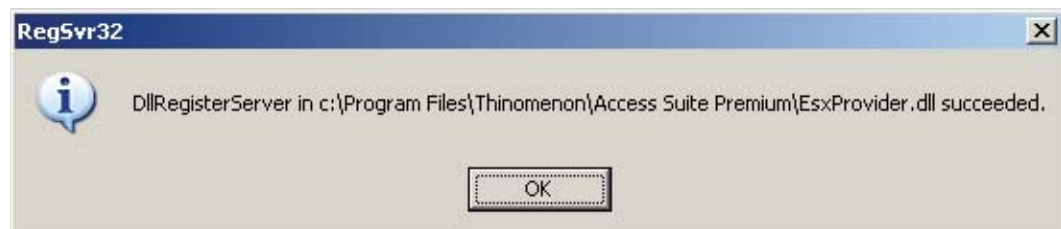
```
regsvr32 full_path_to_EsxProvider.dll
```

and then hit the Enter key.

For example, if Thinomenon Access Suite was installed by default to system disk C the command will look like:

```
regsvr32 C:\Program Files\Thinomenon\Access Suite Premium\EsxProvider.dll
```

In case the operation was successful, you'll get the following message:



After that VMware ESXi/VMware vCenter datacenter can be added to Enterprise Management Console.

8 Appendix C

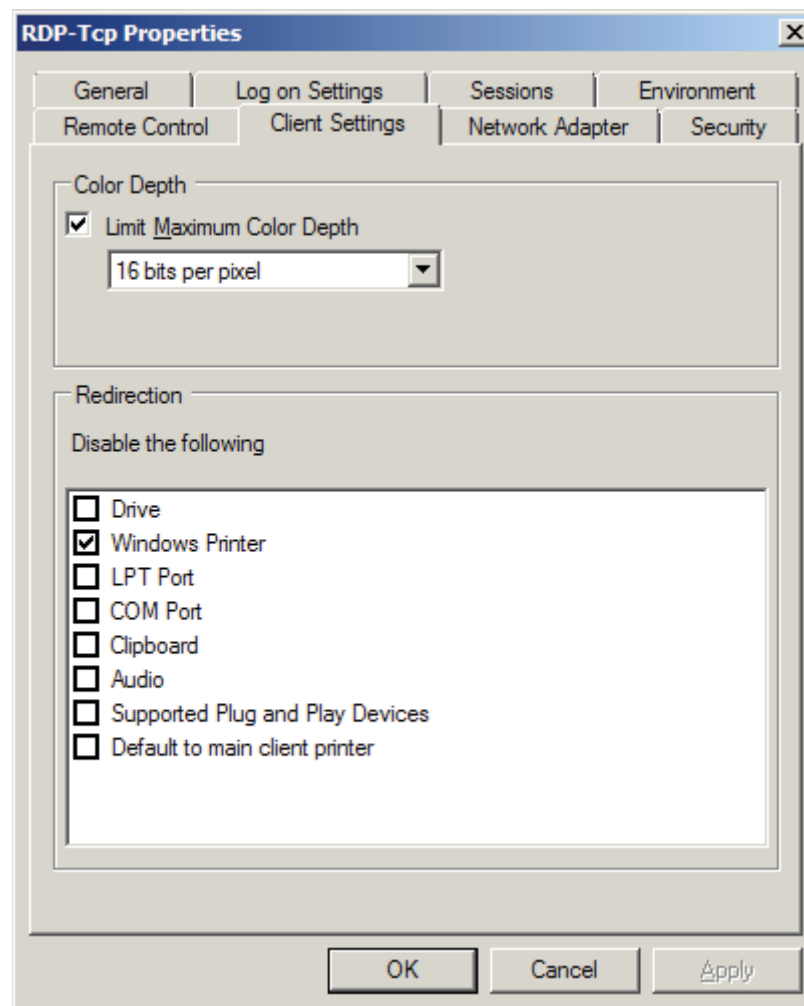
RDP-Tcp properties of Terminal Servers

There are some restrictions set for Terminal Server, which can influence quality and features in remote sessions launched from this server.

To check whether these restrictions are set, go to

Start menu -> Administrative Tools-> Terminal Services -> Terminal Services Configuration.

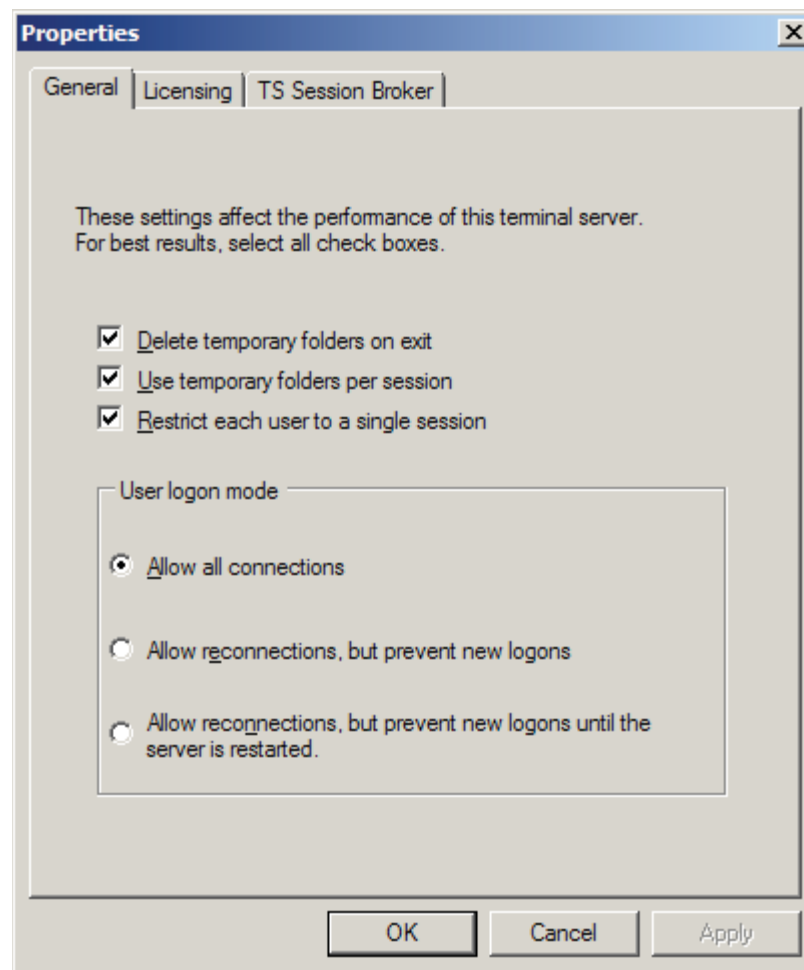
Right-click RDP-Tcp and select ***Properties->Client Settings*** tab



If ***Limit Maximum Color Depth*** option is turned on, remote session won't have more color depth value than is specified.

Also some features such as audio, printers, drives can be disabled from Client settings.

Restrict each user to a single session option defines whether only one or more remote sessions can be launched by the same user.



9 Appendix D

Filtering by users and how to make user/group be present in EMC filtering list

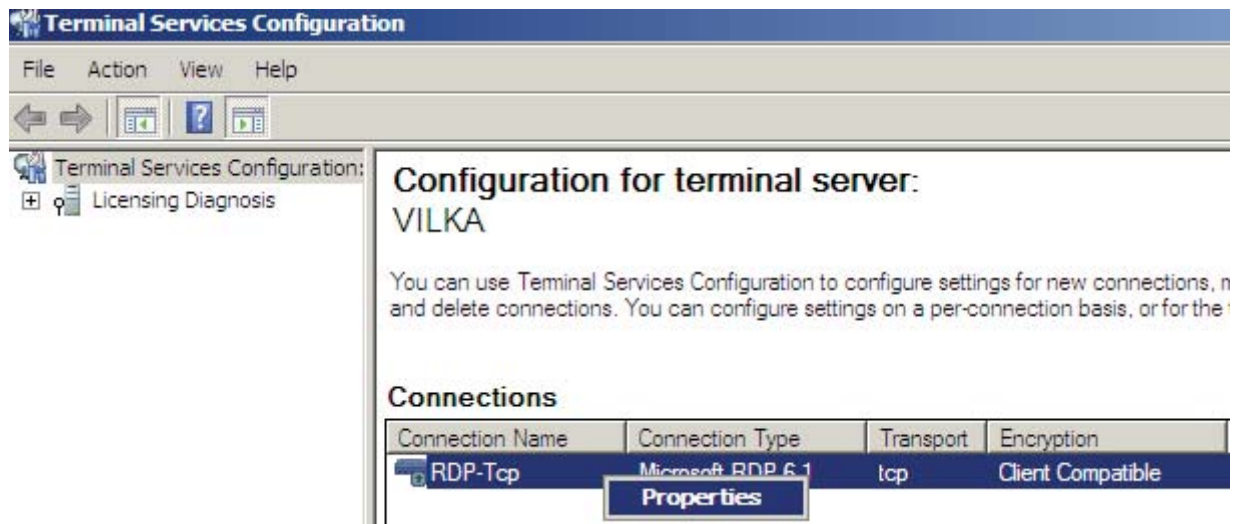
To make user/group be present in EMC Filtering list the following preconditions have to be met:

Security permission in RDP-Tcp properties with *Logon access* granted;

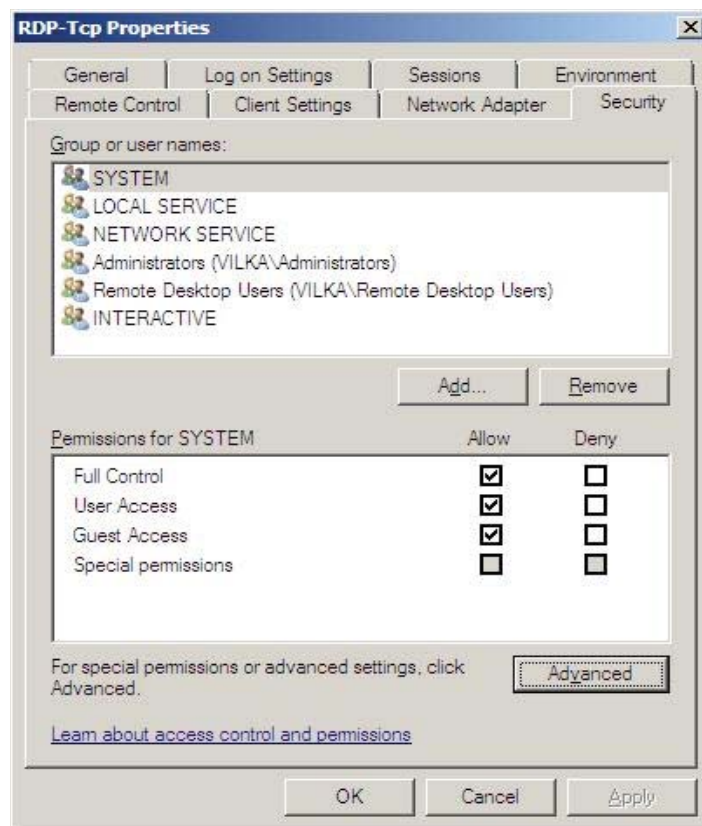
Allow log on through Terminal Services policy granted;

To set the security permissions we need to open RDP-Tcp properties dialog of Member Server.

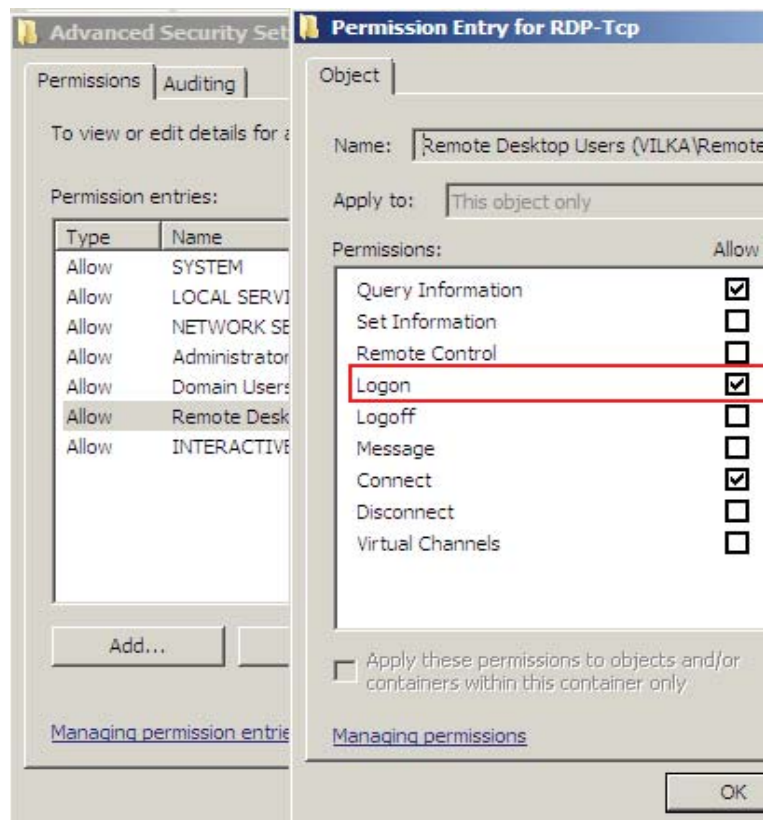
This dialog is available from *Administrative Tools -> Terminal Services -> Terminal Services Configuration*



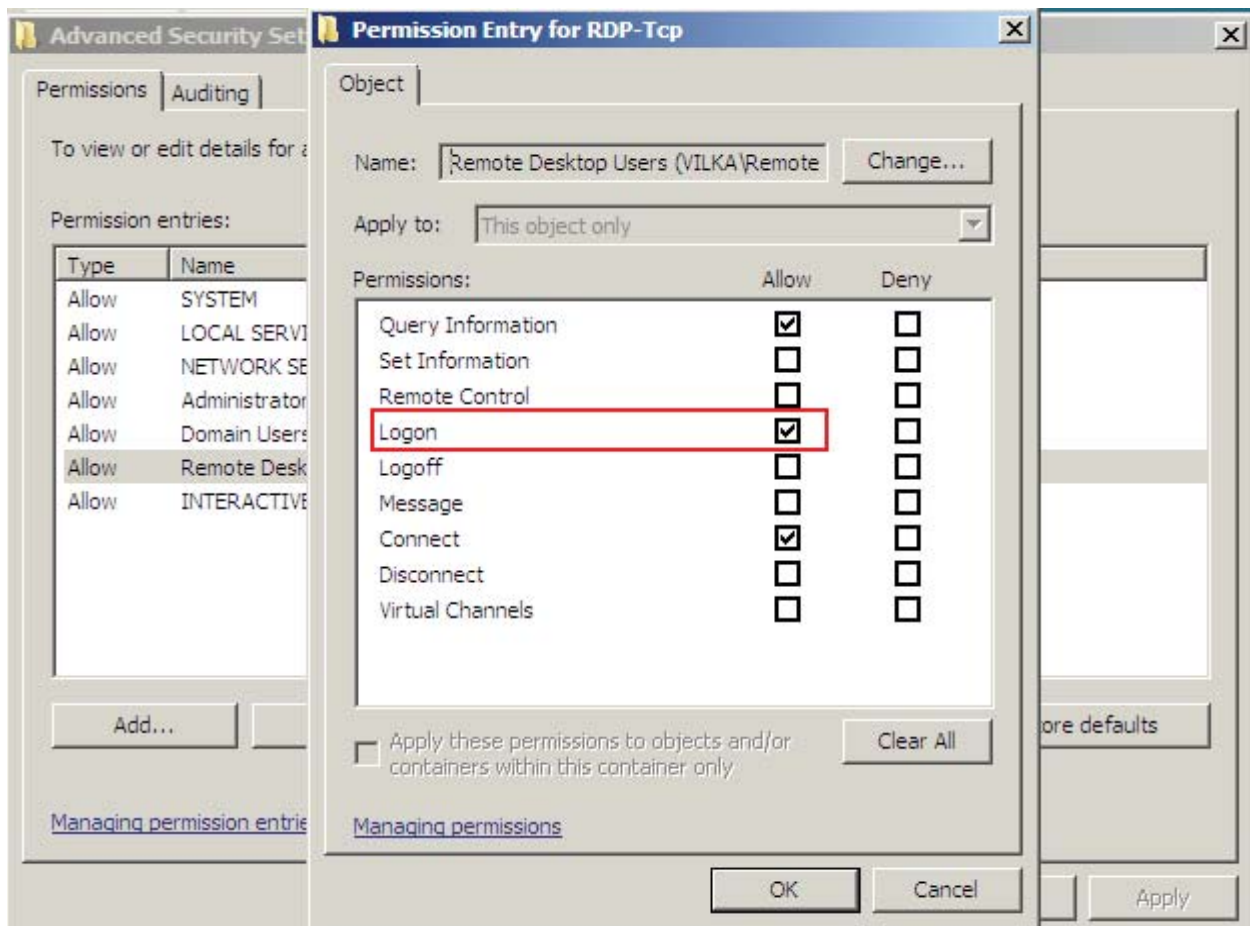
Open *Security* tab of *RDP-Tcp properties* in case of Windows Server 2008



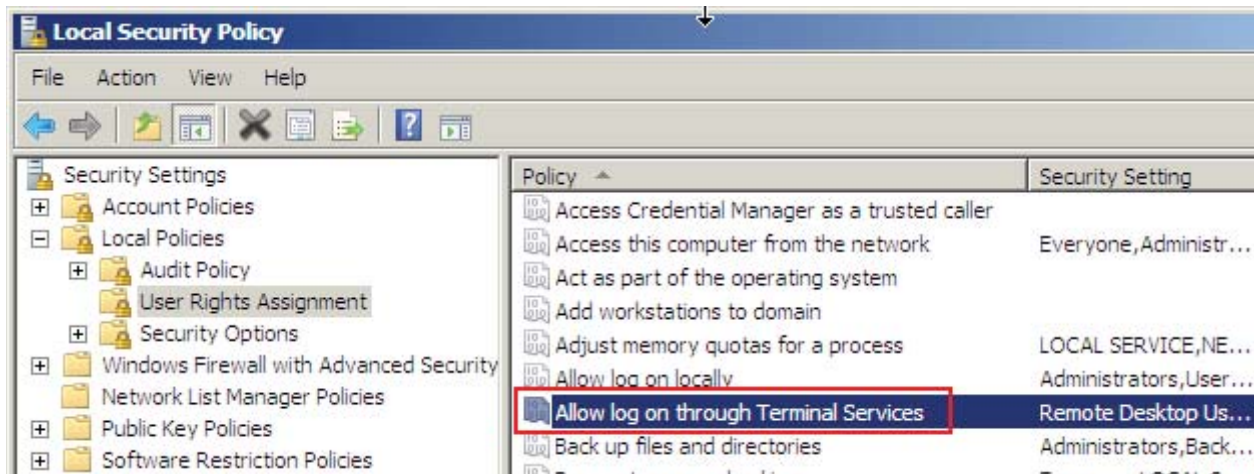
or *Permissions* tab in case of Windows Server 2003



Add users or groups there and allow the *Logon* option in the *Advanced security settings* of *RDP-Tcp*



To be sure that *Allow log on through Terminal Services* policy is granted for user/group check it in *Administrative Tools -> Local Security Policy -> Local policies -> User Rights assignment*



Users/groups that have both mentioned permissions appear in the Filtering list in EMC.

NT Authority groups (SYSTEM, NETWORK SERVICE etc) are ignored.